2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC)

Summary Report

March 14, 2013

TABLE OF CONTENTS

List of Tables

List of Figures

Executive Summary

The National Initiative for Cybersecurity Education (NICE) partnered with the Federal Chief Information Officer's (CIO) Council to develop and distribute the 2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC). NICE evolved from the Comprehensive National Cybersecurity Initiative (CNCI) Initiative 8-Expand Cyber Education, to develop a technologically-skilled and cyber-savvy workforce with the right knowledge and skills. The ITWAC was developed to collect workforce data that would help identify the composition and capabilities of the federal civilian cybersecurity workforce. The assessment can help federal departments and agencies:

- Understand the scope of the cybersecurity workforce pipeline;
- Establish a baseline of current cybersecurity capabilities and proficiencies among the Federal workforce; and
- Identify the general training needs of the cybersecurity workforce.

The ITWAC is similar to the 2011 Information Technology Workforce Capability Assessment (ITWCA), conducted by the Federal CIO Council, and is largely based on the National Cybersecurity Workforce Framework (the Framework).[1] The Framework was developed by NICE using existing cybersecurity research, such as the Federal CIO Council Matrix Project.

A web-based, voluntary, and anonymous self-assessment of proficiency across cybersecurity competencies[2] (referred to as Specialty Areas in the Framework and the ITWAC), the ITWAC was available to participating federal organizations from October 22, 2012, through November 16, 2012, and to the Department of Defense (DoD) from January 15, 2013 through January 31, 2013.

A total of 22,956 participants from 52 federal departments and agencies completed the ITWAC. The Department of Homeland Security (DHS) had the most participants (35.76%) followed by Department of Agriculture (USDA) (13.68%), and Department of Navy (DON) (11.38%).

The ITWAC collected participant demographic information, including pay grade, occupational series, age range, retirement eligibility, work experience, education, and certifications. The assessment also asked participants to provide information that would provide insight on cybersecurity workforce capabilities. This part of the assessment

[1] The National Cybersecurity Workforce Framework (the Framework) outlines 31 functional work specialties within the cybersecurity field. It provides a common understanding of, and lexicon, for cybersecurity work and groups similar types of work into categories and Specialty Areas. http://csrc.nist.gov/nice/framework/

[2] A competency is, "a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to successfully perform work roles or occupational functions." http://apps.opm.gov/ADT/Content.aspx?page=1-03&JScript=1.

included responding to questions regarding time spent working in the 31 Framework Specialty Areas, proficiency in the Specialty Areas, and workforce training needs.

The report found that the typical ITWAC participant is in a position assigned to the General Schedule (GS) - 2210 Information Technology Management occupational series and aligned to the Security parenthetical title. These individuals are typically between the ages of 51 and 55, have more than 10 years of public sector experience, and have more than 10 years of additional service to reach retirement eligibility.

Additionally the report found the following:

- The GS-11 to GS-13 pay grade range accounted for the largest percentage of assessment participants (60.98%).
- The 2210 Information Technology Management occupational series accounted for the largest percentage of assessment participants (30.48%). Participants from this series also spend the most of their time in the Framework Specialty Areas.
- The majority of ITWAC participants (78.50%) are above the age 40. Participants in the 30 and younger age range accounted for 5.15% of the population responding to the assessment.
- Participants indicated a strong need for training in the following Framework Specialty Areas:
    - **Information Assurance (IA) Compliance**
    - **Vulnerability Assessment and Management**
    - **Knowledge Management**

The purpose of the ITWAC is to provide a current snapshot of the federal civilian IT workforce with cybersecurity duties and responsibilities. The data derived from this assessment can serve as a starting point for examining current cybersecurity workforce skills, determining skill gaps, and identifying training to mitigate these gaps. Federal departments and agencies can use the data to support strategic workforce development or talent management activities, such as workforce planning and professional development.

1. INTRODUCTION

1.1 The Emerging Need for Cybersecurity

Many aspects of the Federal Government are supported by electronic information systems and networks. Without the use of this technology, it would be nearly impossible for federal organizations to carry out their missions. Furthermore, inadequate security measures can result in significant risk to, or breach of, information that affects a wide range of government operations, including those relating to critical infrastructures and national security.

In recent years, cyber-attacks have been growing exponentially and affecting the Federal Government, corporations, and individual citizens without discrimination. Since taking office, President Obama has noted that developing effective cybersecurity measures and capabilities is one of the most serious economic and national security challenges we face today as a nation.[3] Exacerbating the issue is the fact that cybersecurity responsibilities are dispersed or duplicated across various federal organizations, many of which have overlapping duties.[4]

According to the 2009 Cyberspace Policy Review, cyber criminals, nation states, and other entities have already stolen hundreds of millions of dollars (as well as intellectual property and sensitive military and intelligence information) from both private industry and the Federal Government. In response to these security breaches, the Federal Government is revising its understanding of cyber risk and vulnerability, and hiring cybersecurity workers to protect internal networks and systems. It is also taking active steps to fortify its cyber space, from infrastructure information to defense networks and homeland intelligence. Now, more than ever, there is a need for a well-trained federal cybersecurity workforce to keep the United States safe from cyber-attacks.

1.2 Cybersecurity is Mission-Critical

Cybersecurity professionals are involved in work that includes the development and application of "…strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[5] Working to this definition, the federal cybersecurity workforce engages in a wide range of activities that are critical to ensuring our nation's Information Technology (IT) networks are secure and protected against all types of cyber threats and liabilities.

---

[3] Comprehensive National Cybersecurity Initiative, 2008. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[4] Cyberspace Policy Review, 2009. http://www.dhs.gov/publication/2009-cyberspace-policy-review.

[5] Cyberspace Policy Review, 2009.

Cybersecurity has become increasingly critical in response to protecting IT systems and cyberspace from cyber-threats. As the field evolves, the challenges facing cybersecurity professionals change rapidly. Cybersecurity professionals must develop and constantly refine the requisite knowledge, skills, and abilities (KSAs) and adapt their application of these KSAs to various work needs. These professionals must also perform at a high level that allows them to identify and initiate quick responses to threats that change frequently in terms of scope and complexity.

Since cybersecurity duties are dispersed across various federal organizations and occupational series, it has been difficult to define the scope of the cybersecurity workforce. There is still ambiguity surrounding the definition of a cybersecurity professional and the competencies required, as well as the training required to adequately satisfy these competencies.[6]

Within the Federal Government, several departments have identified cybersecurity-related workforce challenges. In September 2009, the Department of Commerce Inspector General reported that the department needed to spend more time on the development and management of its cybersecurity staff. In March 2011, the Commander of the U.S. Cyber Command stated that military personnel were not sufficiently equipped to address the current and future cybersecurity threats to the Nation's infrastructure.[7]

1.3 The IT Workforce Assessment for Cybersecurity (ITWAC)

To ensure that the cybersecurity workforce is properly equipped to respond to threats to the Nation's cyberspace, it is important to first understand the current environment of the federal IT workforce, specifically the community that performs cybersecurity functions. The Federal Chief Information Officers (CIO) Council developed the IT Workforce Capability Assessment (ITWCA) to gather data on the composition and training needs of the federal IT workforce as well as to provide departments and agencies with this data in order to make informed human capital decisions.[8]

The ITWCA was conducted in 2003, 2004, 2006, and 2011 and focused on the 2210 Information Technology Management occupational series workforce. For the 2011 ITWCA, it was updated to include a supplemental assessment of the cybersecurity workforce. Assessment participants (who indicated they perform cybersecurity activities) were asked to rate their proficiency on the cybersecurity technical competencies identified in the Office of Personnel Management's (OPM) cybersecurity competency

[6] The Government Accountability Office (GAO) Partnership for Public Service (PPS) reported that, across the Federal Government, agencies cannot readily identify the size and composition of their cybersecurity workforces.

[7] Government Accountability Office. *Cybersecurity Human Capital - Initiatives Need Better Planning and Coordination*. November, 2011. http://www.gao.gov/new.items/d128.pdf.

[8] The Federal CIO Council is the principal interagency forum on federal agency practices for IT management. The CIO Council's mission is to "improve practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal Government information resources." CIO.gov homepage. http://cio.gov/.

model. They were also asked to identify cybersecurity-related competencies in which they required training to better serve their organizations.

In an effort to further identify the composition and capabilities of the federal IT civilian workforce executing cybersecurity responsibilities, the Federal CIO Council and the National Initiative for Cybersecurity Education (NICE) partnered to develop and distribute the IT Workforce Assessment for Cybersecurity (ITWAC).[9] The objectives of the assessment are to help federal departments and agencies:

- Identify federal employees with cybersecurity job responsibilities,
- Establish a baseline of current cybersecurity capabilities and proficiencies among the Federal workforce, and
- Understand the scope of the cybersecurity workforce pipeline.

The ITWAC also provides workforce data that supports NICE-sponsored cybersecurity training, workforce planning, and professional development activities. Departments and agencies can use ITWAC data to support targeted activities related to building the capabilities of their cybersecurity workforce. Ultimately, data acquired from the ITWAC can serve as a basis for future workforce development initiatives.

[9] NICE is led by the National Institute of Standards and Technology (NIST) and comprised of over 20 federal departments and agencies. It is a coordinated effort focused on cybersecurity awareness, education, training, and professional development.

2. SCOPE AND METHODOLOGY

The ITWAC is a voluntary and anonymous self-assessment that quantifies participant proficiency across cybersecurity competencies (referred to as Specialty Areas in the Framework and the ITWAC). The target participant population of the ITWAC was the federal IT civilian workforce with cybersecurity job duties and responsibilities. Contractor personnel were not included in the assessment because deployment time constraints were insufficient to satisfy the legal and contractual hurdles that surround this population. Additionally, active duty military members were not considered as an ITWAC target population.

The assessment participants responded to a series of questions categorized into seven sections: Time Spent in Specialty Areas, Proficiency Ratings, Work Experience, Training Needs, Education, Certifications, and Demographics. Table 1 provides a summary of each section:

Table 1: ITWAC Sections

Section	Description
Time Spent in Specialty Area	Captures the average time that participants spend in each cybersecurity Specialty Area
Proficiency Ratings	Captures participants' average proficiency rating in each of the 31 Specialty Areas
Work Experience	Identifies participants' various levels of work experience in Federal Government, SLTT, private sector, and academia
Training Needs	Indicates Specialty Areas in which participants felt more training would be beneficial to them in their current role
Education	Allows participants to indicate their academic degrees and majors
Certifications	Captures the certifications acquired by participants relevant to cybersecurity
Demographics	Collects participants' demographic information

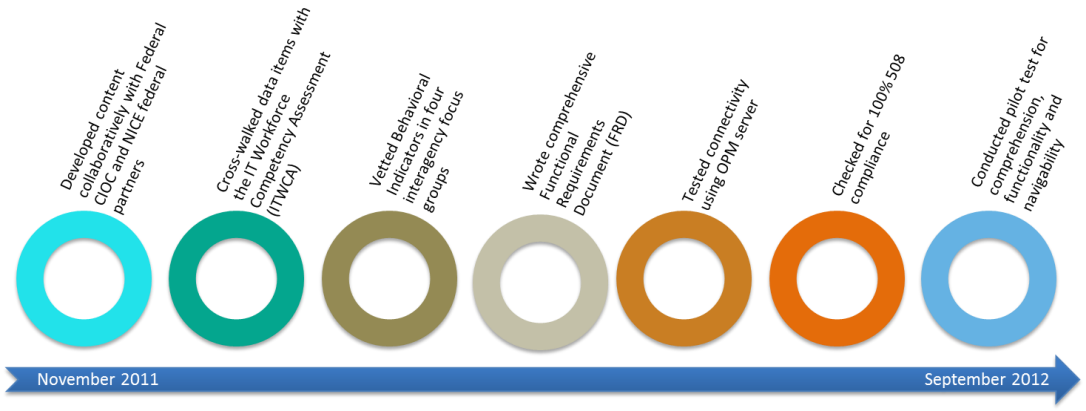
2.1 Assessment Design

The ITWAC is based largely on the 31 Specialty Areas identified in the Framework developed by NICE. The Framework was created to provide a common language and taxonomy for cybersecurity work across the Federal Government. It identifies and defines 31 common functional Specialty Areas within the cybersecurity field and organizes them into seven high-level categories. *Figure 6 in Appendix B displays a visual representation of the Framework.* The Framework development began in 2010, and has been available for public review on the NIST website since September 2011. In August 2012, NICE released the official Framework (Version 1.0) on the NIST website.

The ITWAC was created using an extensive and rigorous methodology. Developers worked to ensure that the assessment related to existing IT-workforce federal survey data,

was relevant to a wide range of departments and agencies, and accommodated users with a variety of functionality and connectivity needs. The ITWAC complied with standard survey best practices, Section 508, and security requirements. Figure 1 illustrates the assessment development process.

Figure 1: ITWAC Development Process



2.2 Workforce Data Collection and Analysis

The ITWAC was administered using the Federal Competency Assessment Tool (FCAT). The FCAT is a survey application used for workforce planning, individual development and career planning. It was selected for the ITWAC because of its role as a common platform for conducting surveys across Federal Government organizations and because it is a platform already owned by the Government. The FCAT has been previously used to survey federal acquisition professionals, human resources professionals and managers. The FCAT also provides a broad set of reports that are used to help understand the demographic profile and cyber expertise of ITWAC respondents.[10]

The ITWAC was available to participating departments and agencies from October 22, 2012, through November 16, 2012.[11] Agency and department Points of Contact (POCs) were provided with outreach material that identified 39 occupational series with cybersecurity duties and responsibilities. Participants assigned to positions in these select occupational series were notified of the opportunity to take the assessment by their department and agencies' designated POCs. Once notified, participants visited the assessment website, where they completed the assessment as an anonymous user. Participants were also provided with a unique 36 digit alpha-numeric code to login and access their assessment at a later time, if they did not complete it in one session. Assessments were considered valid when all required sections were completed and the

[10] *2011 Information Technology Capability Assessment Survey Results Report*. May 2011.
[11] The ITWAC was re-launched for DoD (including the Headquarters, Air Force, Army and Navy) from January 15, 2013 through January 31, 2013.

participant acknowledged completion by clicking the "Submit" button. Incomplete assessment records were not included in the analysis and were not supplied to the participating departments and agencies. *Appendix D displays all questions in the ITWAC*.

The ITWAC displays participant data in aggregate form to protect personally identifiable information (PII) of the participants, as well as to ensure anonymity.

At the conclusion of the ITWAC, department and agency POCs were provided access to the online ITWAC tool to analyze their department and agencies' participant data. This is the same tool the ITWAC developers used to capture participant responses; however, agency POCs can only view results for their specific IT workforce. Furthermore, the online tool gives agency POCs the functionality to view each of the assessment sections in the form of exported reports. Departments and agencies also have the option of filtering the data for custom analysis using the following custom filters:

- Home agency/department,
- Occupational series,
- Parenthetical title,
- Pay grade,
- Employee type,
- Supervisory status,
- Retirement eligibility, and
- Demographics (gender, age, ethnicity, race/national origin, disability status, and veteran status), education, and certifications.

3. ITWAC Findings – Workforce Composition

A total of 22,956 individuals participated in the ITWAC. The participants represented 52 federal departments and agencies with cybersecurity workforces. The call for participation was originally distributed to over 80 departments and agencies in September 2012 which, in turn, sent the assessment to over 200,000 of their IT professionals considered to have cybersecurity responsibilities. *Appendix C – Table 14 displays the 52 departments and agencies that participated in the ITWAC*.

The Federal Government organization with the highest participation was the Department of Homeland Security (DHS), with more than a third of the participants completing the assessment, followed by the Department of Agriculture (USDA). Table 2 shows the 10 departments and agencies with the most ITWAC participants.

Table 2: Federal Agency Participation

Department/Agency	Number	Percentage of Assessment Population
Department of Homeland Security	8,208	35.76%
Department of Agriculture	3,141	13.68%
Department of Navy	2,612	11.38%
Department of Defense – Headquarters	1,856	8.09%
Department of Army	1,509	6.57%
Department of Commerce	1,497	6.52%
National Aeronautical and Space Administration	627	2.73%
Department of the Interior	529	2.30%
Department of the Air Force	463	2.02%
Small Business Administration	444	1.93%

3.1 Pay Grade

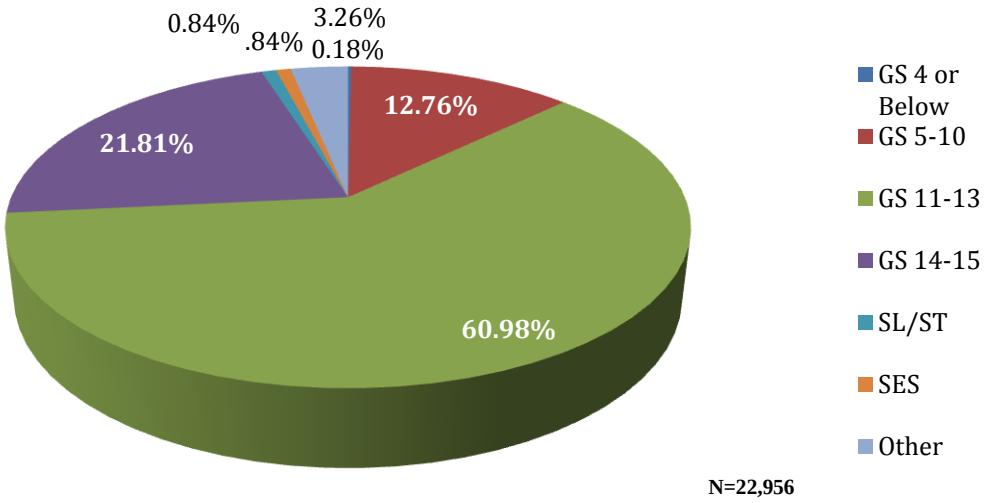
Key Findings
• 60.98% of the assessment population belongs to the GS-11 to GS-13 pay grade • 21.81% of the assessment population belongs to the GS-14 to GS-15 pay grade

The ITWAC required participants to identify themselves with their government pay grade. Options included pay grades within the General Schedule (GS), Senior Executive Service (SES), and Senior Leadership and Scientific and Professional (SL/ST).[12] For final reporting purposes, GS pay grades were grouped into four GS ranges. The GS-11 to GS-

[12] The SL/ST pay grade is an SES-equivalent pay grade for recognized scientific and technical authorities.

13 range accounted for the largest number of assessment participants, followed by the GS-14 to GS-15 range and the GS-5 to GS-10 range, respectively. The GS-4 and below range accounted for the lowest number of assessment participants. When appropriate, ITWAC participants could select "Other" and provide an open-ended response. The H and I band pay grades, which are employed by the Transportation Security Administration (TSA), were the most common open-ended responses to the "Other" pay grade question. Figure 2 displays the participant distribution by pay grade.

Figure 2: Participation by Pay Grade



3.2 Occupational Series

Key Findings
• The 2210 occupational series accounted for the largest assessment population at 30.48%. • A large number of participants indicated belonging to an occupational series not included in the list of response options.

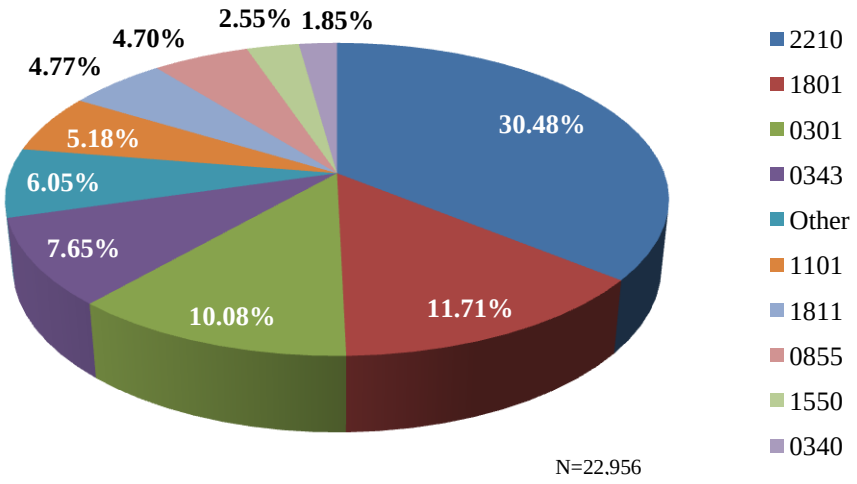
Participants were required to select their occupational series from a list of 39 options. *The list of OPM occupational series options appears in Appendix C – Table 15*. From these options, the 2210 Information Technology Management occupational series accounted for the largest number of participants who completed the ITWAC.

Over 1,300 participants stated they belong to an occupational series other than those listed in the assessment. Upon examining the open ended responses for "Other" occupational series, there was no series with a majority of responses. Most participants stated "N/A" or "Unknown." Table 3 identifies the 10 most common occupational series (with the option of "Other" included) among participants who completed the ITWAC. These occupational series also appear as percentages in Figure 3.

Table 3: Participation by Occupational Series

Occupational Series	Number	Percentage
2210 - Information Technology Management	6,997	30.48%
1801 - General Inspection, Investigation, Enforcement, and Compliance	2,689	11.71%
0301 - Miscellaneous Administration and Program	2,315	10.08%
0343 - Management and Program Analysis	1,755	7.65%
Other (i.e., other occupational series not listed in response options)	1,388	6.05%
1101 - General Business and Industry	1,188	5.18%
1811 - Criminal Investigation	1,095	4.77%
0855 - Electronics Engineering	1,080	4.70%
1550 - Computer Science	586	2.55%
0340 - Program Management	425	1.85%

Figure 3: Most Common Occupational Series



3.3 Parenthetical Titles - 2210 Information Technology Management Occupational Series

ITWAC participants who identified themselves as belonging to the 2210 series were required to select a primary parenthetical title and an optional secondary parenthetical title. Participants could select "None" if they were not assigned a parenthetical title or were unsure of their parenthetical title.

The majority of the 2210 series participants selected Security as their parenthetical title. Although most positions classified to the 2210 series receive a primary parenthetical title, many participants selected "None" for parenthetical title. Likewise, in the 2011 ITWCA, a high percentage of the cybersecurity workforce was not associated with a primary or

secondary parenthetical title. Table 4 displays the 2210 series parenthetical titles and participant breakdown by number, the percentage of the parenthetical title as it relates to the 2210 series, as well as the percentage of the parenthetical title as it relates to the total assessment population.

Table 4: Participation by 2210 Series Parenthetical Title

Parenthetical Title	Number	Percentage of 2210 Occupational Series	Percentage of Assessment Population
Security	1277	18.25%	5.56%
None	1047	14.96%	4.56%
Customer Support	817	11.68%	3.56%
Systems Administration	777	11.10%	3.38%
Applications Software	730	10.43%	3.18%
Policy and Planning	691	9.88%	3.01%
Systems Analysis	612	8.75%	2.67%
Network Services	391	5.59%	1.70%
Data Management	317	4.53%	1.38%
Enterprise Architecture	152	2.17%	0.66%
Operating Systems	105	1.50%	0.46%
Internet	81	1.16%	.035%

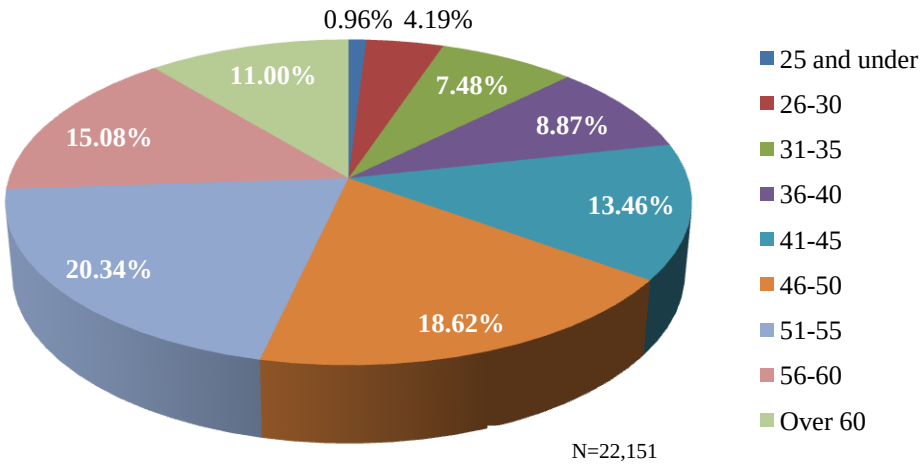
3.4 Age Distribution

Key Findings
• Majority of participants (78.50%) are above age 40. • The 30 and younger range only accounts for 5.15% of the age response population.

ITWAC participants had the opportunity to indicate their ages from a selection of age ranges. Each age range option covered five years, with the exception of the "25 and under" and "Over 60" choices. The age range with the largest number of participants was 51-55, while the "25 and under" range had the lowest participation.

The data suggests that the majority of the participants are above the age of 40, with most being closer to the retirement age threshold. While specific factors (e.g., years of experience at hire) may be influencing the average age of a department or agency's workforce, this data indicates potential risk to the current and future pipeline of cybersecurity professionals. An aging cybersecurity professional population could lead to a manpower shortage in the federal cybersecurity field (particularly in management and leadership positions). Figure 4 displays the age range distribution of the participants.

Figure 4: Participant Age Range Distribution

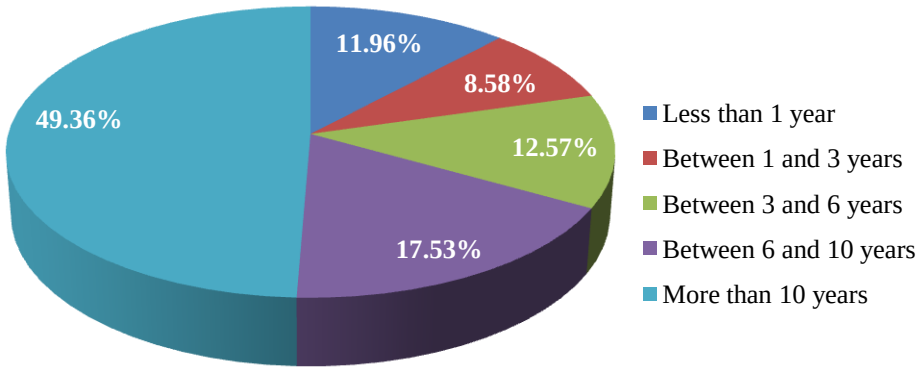


3.5 Retirement Eligibility

Key Findings
• 11.96% of participants are eligible for retirement in less than a year. • 20.54% of participants are eligible for retirement in the next three years.

Participants could voluntarily identify their retirement eligibility status as it relates to requirements set forth by OPM. Although the majority of participants (above the age of 40) indicated having more than 10 years left before reaching retirement eligibility, there are still a significant percentage of participants eligible for retirement within the year. This potential loss of experienced personnel can lead to a shortage of skilled employees and place a greater burden on the existing cybersecurity staff, as well as seriously affect the daily operations of the Federal Government. It is important to point out that, even though an individual may be eligible for retirement, it does not necessarily mean this person will be retiring right away. Figure 5 displays the retirement eligibility distribution of the ITWAC participants.

Figure 5: Participant Retirement Eligibility



N=22,338

Table 5 displays ITWAC participant retirement eligibility by pay grade. The GS-11 to GS-13 pay grade has the largest number of participants who are eligible for retirement in less than one year. The SL/ST pay grade has the next highest percentage.

Table 5: Retirement Eligibility of Participants

Pay Grade	< 1 Year	1-3 Years	3-6 Years	6-10 Years	> 10 Years
GS 4 and below	1	6	8	6	18
GS 5-10	240	202	294	399	1,684
GS 11-13	1,479	1,087	1,675	2,414	7,002
GS 14-15	820	527	704	949	1,905
SL/ST	9	6	5	8	10
SES	55	26	37	29	40
Other	68	63	85	110	367

3.6 Work Experience

Key Findings
• The majority of participants have spent most of their careers in the Federal Government, although not specifically within the cybersecurity specialty.

Participants had the opportunity to indicate the number of years of cybersecurity experience they acquired in Federal Government, State, Local, Tribal, and Territorial (SLTT) government, private sector, and academia. They could also indicate if they worked for the Federal Government in a capacity other than cybersecurity. Table 6 displays the percentages of the ITWAC participants who have work experience in these sectors. The work experience of the participants consists predominantly of federal service. After examining the age range of the participants, it is not surprising that the

majority has more than 10 years of work experience, be it in government, the private sector, or academia. The majority **(**68.63%**)** of the participant population indicated that they have more than 10 years of experience in the federal workplace in any capacity. The smallest percentage of ITWAC participants indicated gaining cybersecurity experience in SLTT government and academia.

Table 6: Participant Work Experience

Cybersecurity Experience	Less than 1 Year	Between 1 and 3 Years	Between 3 and 6 Years	Between 6 and 10 Years	More than 10 years
Federal	4.69%	9.61%	8.48%	7.84%	14.62%
SLTT	1.46%	1.76%	1.25%	0.86%	1.51%
Private Sector	2.21%	4.68%	3.62%	2.72%	3.78%
Academia	2.27%	3.08%	1.30%	0.47%	0.51%
Federal in any Capacity	1.61%	5.79%	9.28%	10.98%	68.63%

3.7 Education

When asked about their education, 17,604 participants indicated that they had received an academic degree. Of those participants, 12,030 identified at least one degree and field of study. 18,703 total degrees were identified. It is important to note that, since the education item in the ITWAC was optional, the overall number of academic degrees is not a true representation of all the degree holding participants. The researchers also noticed that many participants only listed their highest degree achieved, rather than every degree they possess; this suggests that the number of total degrees may be lower than the data provided here (e.g., a participant only identified his or her Master's degree and did not include the Bachelor's degree earned previously; therefore, total degree count would be 1 instead of 2).

The most common majors for each degree type are displayed in Table 7. With the exception of the doctorate degree, Business Administration and Management was the most popular field of study. Most participants with doctorate degrees indicated that law (Juris Doctorate) was their field of study. The participants indicated a wide variety of backgrounds; however, business, government-related majors, and engineering/computer majors are the most common fields of study.

Table 7: Participant Field of Study (Most Common)

Degree/Major	Numbers
Doctorate	
Law (Juris)	152
Engineering	67
Science	46
Management	15

Degree/Major	Numbers
Philosophy	14
Master's	
Business Administration & Management	781
Information Technology	326
Computer Science	243
Public Administration	242
Electrical Engineering	212
Bachelor's	
Business Administration & Management	955
Electrical Engineering	734
Computer Science	702
Criminal Justice	432
Computer and Information Sciences/System	412
Associate's	
Business Administration and Management	233
General Studies	137
Business, General	130
Information Technology	123
Computer and Information Sciences/Systems	100

3.8 Certifications

The ITWAC provided participants an opportunity to identify any certifications they have acquired during their professional experience.[13] The greatest percentage of participants responding to this item had certifications in the Technology category, followed by the Information Security category. Since the certification item in the ITWAC was optional, the overall number of certifications may not be a true representation of all the certification-holding participants.

Table 8 displays the number of participants with certifications from the respective certification categories. The most popular certification identified was the Computing Technology Industry Association (CompTIA) - Security +, followed by the International Information Systems Security Certification Consortium, Inc. (ISC)^2 - Certified Information Systems Security Professional (CISSP). The top five certifications by category are displayed in Table 9.

[13] The list of certification options in the 2012 ITWAC was developed using 2011 ITWCA information.

Table 8: Participant Certification Breakdown by Category

Certification	Numbers
Contracting	2,275
Information Security	1,458
Technology	1,353
Other	796

Table 9: Participant Certifications (Most Common)

Certification Category	Numbers
Contracting	
Federal Acquisition Certification - Contracting Officer Technical Representative (FAU - COTR)	213
Project Management Institute (PMI) - Project Management Professional (PMP)	193
CIA Contracting Officer Technical Representative (COTR) - Level I	171
Defense Acquisition Workforce Improvement Act (DAWIA) Systems Planning, Research, Development and Engineering - Systems Engineering (SPRDE - SE) - Level III	147
Defense Acquisition Workforce Improvement Act (DAWIA) Information Technology (IT) - Level I	128
Information Security	
International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ - Certified Information Systems Security Professional (CISSP)	953
E-Commerce-Council - Certified Ethical Hacker	183
Certified Information Security Manager (CISM)	83
Certified Information Systems Auditor (CISA)	80
Security Leadership, MGMT 512 (GSLC)	78
Technology	
Computing Technology Industry Association (CompTIA) - Security +	1,503
Computing Technology Industry Association (CompTIA) - A +	529
Computing Technology Industry Association (CompTIA) - Network +	453
Microsoft Certified Professional (MCP)	453
Cisco Certified Network Associate (CCNA)	235

3.9 Typical Participant Profile

Table 10 depicts the profile of the typical ITWAC participant, based on the highest frequency of responses in each category. It shows the most common demographic information for a cybersecurity federal employee participating in the ITWAC. The typical participant profile of the cybersecurity worker captured in the 2011 ITWCA findings is also included in the table to provide a comparison of both efforts.

Table 10: Typical Participant Profile

Participant Profile	2012 ITWAC	2011 ITWCA
Series	2210 Information Technology Management	2210 Information Technology Management
Primary Parenthetical Title	Security	Security
Pay Grade	GS-13 or equivalent	GS-12 or equivalent
Years of IT Experience	Over 10 years Federal Government	Over 20 years public sector with less than 1 year private sector
IT Certification	Computing Technology Industry Association (CompTIA) - Security +	Information Systems Security
Degree/Major	Bachelor's in Business Administration and Management	N/A
Age Range	51-55 (20.34%)	46-50 (20.5%); 51-55 (20.4%)
Retirement Eligibility	More than 10 years	11-20 years

When comparing the participant profile of the 2012 ITWAC to the 2011 ITWCA, there are several similarities. Both assessments indicate that the typical participant is from the 2210 occupational series, is aligned to the Security parenthetical title, is between the ages of 51 and 55, has more than 10 years of public sector experience, and has more than 10 years of service to reach retirement eligibility.

4. ITWAC Findings – Workforce Capabilities

The main focus of the ITWAC was to identify the composition and capabilities of the federal IT workforce executing cybersecurity responsibilities. In addition to capturing the demographics (i.e., composition) of the assessment population, the ITWAC captured:

- Time that participants report spending in the Framework Specialty Areas,
- Participant proficiency in the Specialty Areas, and
- Specialty Areas participants indicated they could enhance through training.

Section 4.1, Time Spent in Specialty Areas, shows the percentage of time that participants report spending in each of the 31 Framework Specialty Areas. This section first shows the time spent in Specialty Areas for the total assessment population. It then shows the time spent in each Specialty Area further broken down by participant pay grade, occupational series, and 2210 series parenthetical titles.

Section 4.2, Specialty Area Proficiency Ratings, displays the average participant proficiency ratings for each Specialty Area. Participants self-assessed their current levels of proficiency in each Specialty Area. In addition, participants indicated the proficiency levels required for someone in their role (optimal proficiency).

Similar to Section 4.1, this section starts by focusing on the average proficiency ratings of the total assessment population. It then shows average proficiency ratings further broken down by participant pay grade, occupational series, and 2210 series parenthetical titles. The occupational series and 2210 series parenthetical titles were also analyzed to determine the percentage of this population that indicated Advanced/Expert proficiency or how many meet/exceed optimal proficiency.

Section 4.3, Training Needs, displays the percentage of assessment participants that indicated training in specific Specialty Areas would be beneficial to performance in their current roles. This section shows the training needs for the total assessment population. It then shows training needs further broken down by participant pay grade, occupational series, and 2210 series parenthetical titles.

4.1 Time Spent in Specialty Areas

Time Spent in Specialty Areas indicates the percentage of time that participants report spending in the 31 Framework Specialty Areas. Time spent was analyzed for the total assessment population, and then broken down by participant pay grade, occupational series, and 2210 series parenthetical titles.

Total Assessment Population

Key Findings
• Participants spend 53.81% of total time in work other than Specialty Areas. • Customer Service and Technical Support accounts for 6.40% of total time.

The total assessment population indicated that they spend the majority of their time performing work in areas other than the 31 Specialty Areas. For work performed in the Specialty Areas, **Customer Service and Technical Support** accounts for the largest percentage of time spent, followed by the **Information Assurance (IA) Compliance** Specialty Area. *Appendix C - Table 25 displays the time spent percentages of the total assessment population.*

Time Spent in Specialty Areas - Pay Grade

Key Findings
• GS-11-13 pay grade has the highest percentage of participants engaging in Specialty Areas (49.48%). • **Customer Service and Technical Support** accounts for a large percentage of time spent across the pay grades. • GS-4 and below pay grade spends 6.56% of their time in **Incident Response**. • SL/ST participants spend 8.97% of their time in Strategic Planning and Policy Development.

The pay grade grouping with the highest percentage of participants engaging in cybersecurity work (as represented by the 31 Specialty Areas) is GS 11-13. Of the Specialty Areas, **Customer Service and Technical Support** is an area where participants spend a substantial amount of time (compared to the other Specialty Areas). This is regardless of participant pay grade. **Incident Response** was the Specialty Area where GS 4 and below pay grade participants indicated spending most of their time. For SL/ST participants, **Strategic Planning and Policy Development** was the Specialty Area where SL/ST participants indicated spending most of their time. *Appendix C – Table 26 displays the full listing of the time spent percentages by pay grade.*

Time Spent in Specialty Areas - Occupational Series

Key Findings
• 2210 series participants spend 79.81% of their time in the Specialty Areas, 14.40% of this time is spent in **Customer Service and Technical Support**. • 43.35% of the 2210 series participants spend all of their time in the Specialty Areas. • 1550 - Computer Science series participants spend 70.07% of their time engaging in work related to the Specialty Areas. • 1811 - Criminal Investigation series participants spend 26.48% of their time in work related to the **Investigation** Specialty Area.

Of the 10 occupational series with the most participants, those in the 2210 series spend most of their time their time in work related to the Specialty Areas. Participants in the 1550 Computer Science series also spend the majority of their time performing work related to the Specialty Areas. *Appendix C -Table 27displays the full listing of the time spent percentages by occupational series*. Note: the occupational series "Other" refers to a category of participants who belonged to an occupational series not listed as an option in the ITWAC, or they didn't know the occupational series to which they belonged.

The occupational series were also analyzed to determine the number of participants spending 100% of their time in the Framework's cybersecurity Specialty Areas, or whose

work could be considered wholly cybersecurity. The 2210 Information Technology Management occupational series had the most participants spending all of their time in cybersecurity Specialty Areas followed by the 1550 Computer Science series. *Appendix C - Table 28 displays the number of participants spending 100% of their time in the Specialty Areas.*

Time Spent in Specialty Areas- 2210 Series Parenthetical Titles

Key Findings
• Participants in the Security parenthetical title spend 93.21% of their time in the Specialty Areas. • Participants in the Systems Administration parenthetical title spend 89.17% of their time in Specialty Areas.

When the 2210 Information Technology Management occupational series was further grouped by 11 OPM parenthetical titles, it was found that participants in certain 2210 parenthetical titles spend larger percentages of their time working in the cybersecurity Specialty Areas. The Security parenthetical title had the highest percentage of participants engaging in work related to the Specialty Areas, followed by the Systems Administration parenthetical title. *Appendix C - Table 29 displays the full listing of time spent percentages by 2210 series parenthetical titles.*

4.2 Average Proficiency Ratings

This section shows the average of participant self-reported proficiency ratings of the Specialty Areas for the total assessment population. It also shows the participant averages by pay grade, occupational series, and 2210 series parenthetical titles.

ITWAC participants self-assessed their current proficiency level in each of the 31 Specialty Areas. In addition, participants indicated the optimal level of proficiency someone should demonstrate in their role. The proficiency scale is displayed in Table 11. This proficiency scale was developed through analysis of existing proficiency scales used by several federal departments (e.g., OPM, Department of Homeland Security, and Department of Defense).

Table 11: Specialty Area - Proficiency Scale

Proficiency Level	Definition
4 – Expert	I have the **expert** knowledge and skills necessary in this Specialty Area for independent use and application in highly complex, difficult, or ambiguous work situations, **or I am an acknowledged authority, advisor, or key resource in this Specialty Area.**
3 – Advanced	I have the **advanced** knowledge and skills necessary in this Specialty Area for independent use and application in complex or novel work situations.
2 – Intermediate	I have the **intermediate** knowledge and skills necessary in this Specialty Area for independent use and application in straightforward, routine work situations with limited need for direction.

Proficiency Level	Definition
1 – Basic	I have the **basic** knowledge and skills necessary in this Specialty Area for use and application in simple work situations with specific instructions and/or guidance.
0 – None	I do not have the sufficient knowledge or skills necessary in this Specialty Area for use in simple or routine work situations. Any awareness, knowledge, or understanding I do have would be considered common, similar to that of a layperson. **Considered "no proficiency" for purposes of accomplishing work.**

Average Proficiency - Total Assessment Population

Key Findings
• The highest average proficiency rating was in the **Customer Service and Technical Support** Specialty Area (2.39). • 73.90% of the total assessment population meets or exceeds optimal proficiency in **Customer Service and Technical Support**. • The lowest percentage of participants (of the total assessment population) meeting/exceeding optimal proficiency was in **Digital Forensics** (56.61%). • The lowest percentage of participants (of the total assessment population) with Advanced or Expert proficiency was in **Cyber Operations** (5.67%).

The average self-assessed proficiency ratings were reported for participants who indicated having at least Basic (level 1) proficiency in the Specialty Areas. This eliminated proficiency ratings of "None" (level 0) of participants who may not be engaging in certain cybersecurity responsibilities, and would therefore, skew the overall average toward zero. The following is a summary of the proficiency findings for the total assessment population:

- The Specialty Area with participants with the highest average proficiency was **Customer Service and Technical Support** Specialty Area, followed by **Systems Requirements Planning** and **Test and Evaluation**.
- The Specialty Area with the most participants meeting or exceeding optimal proficiency was **Customer Service and Technical Support,** followed by **Education and Training**, **Systems Development**, and **Systems Requirements and Planning**.
- The Specialty Area with the lowest percentage of assessment participants meeting or exceeding optimal proficiency was **Digital Forensics,** followed by **Threat Analysis** and **All Source Intelligence**.
- The **Customer Service and Technical Support** Specialty Area accounted for the highest percentage of participants with either Advanced or Expert proficiency, followed by **Systems Requirements Planning** and **Test and Evaluation**.

- The Specialty Areas with the lowest percentage of assessment participants with Advanced or Expert proficiency were **Cyber Operations**, **Threat Analysis**, and **Targets**.

Appendix C – Table 25 displays the average proficiency ratings and percentages of the total assessment population.

Pay Grade

Key Findings
• Across the pay grades, **Customer Service and Technical Support** and **Systems Requirements Planning** Specialty Areas had high average proficiency ratings. • SL/ST participants attributed the highest average proficiency rating to the **Systems Requirements Planning** Specialty Area (2.88).

In addition to reporting the average proficiency levels of the Specialty Areas for the total assessment population, proficiency levels were also reported by participants' pay grades. Table 12 shows the resulting averages when level 0 proficiency is removed as a response option from the proficiency scale. For each pay grade, the two cybersecurity Specialty Areas with the highest proficiency levels are displayed in Table 12.

Table 12: Average Proficiency Ratings - Pay Grade

Pay Grade	Specialty Area (Top Two)	Average Proficiency Rating
GS 4 and below	Test and Evaluation	2.33
	Systems Requirements Planning	2.11
GS 5-10	Customer Service and Technical Support	2.19
	System Administration	1.95
GS 11-13	Customer Service and Technical Support	2.47
	Systems Requirements Planning	2.28
GS 14-15	Systems Requirements Planning	2.43
	Customer Service and Technical Support	2.28
SES	Strategic Planning and Policy Development	2.29
	Systems Requirements Planning	2.11
SL/ST	Systems Requirements Planning	2.88
	Strategic Planning and Policy Development	2.74
	Systems Security Architecture	2.74
Other	Customer Service and Technical Support	2.19
	Systems Requirements Planning	2.11

For SL/ST participant, the highest average proficiency rating was in the **Systems Requirements Planning** Specialty Area. The **Customer Service and Technical Support** Specialty Area had high proficiency ratings across the pay grades. At the SES and SL/ST levels, **Systems Requirements Planning** and **Strategic Planning and Policy**

Development Specialty Areas have the highest proficiency ratings. *Appendix C - Table 30 displays the full listing of average proficiency ratings by pay grade.*

Average Proficiency - Occupational Series

Key Findings - Average Proficiency
• Participants in the 2210 Information Technology Management occupational series had the highest average proficiency rating for **Customer Service and Technical Support** (2.83). • Participants from six occupational series had high proficiency ratings for **Systems Requirements Planning.** • Participants from five occupational series had high proficiency ratings for the **Customer Service and Technical Support** Specialty Area.

Average proficiency ratings from the 10 occupational series with the most participants were also reported. *Refer to Appendix C - Table 24 for the full title of each occupational series.* For each occupational series, the two Specialty Areas with the highest reported levels of proficiency are displayed in Table 13.

Table 13: Average Proficiency Ratings by Occupational Series

Occupational Series	Specialty Area (Top Two)	Average Proficiency Rating
2210	Customer Service and Technical Support	2.83
	Systems Requirements Planning	2.59
1801	Investigation	2.08
	Education and Training	1.91
0301	Customer Service and Technical Support	1.93
	Systems Requirements Planning	1.87
0343	Customer Service and Technical Support	1.93
	Education and Training	1.90
1101	Strategic Planning and Policy Development	1.65
	Education and Training	1.65
	Data Administration	1.64
	Test and Evaluation	1.64
	Systems Development	1.64
	All Source Intelligence	1.64
	Customer Service and Technical Support	1.64
1811	Investigation	2.42
	Digital Forensics	1.89
0855	Test and Evaluation	2.21
	Systems Requirements Planning	2.20
1550	Systems Requirements Planning	1.75

Occupational Series	Specialty Area (Top Two)	Average Proficiency Rating
	Systems Development	1.65
0340	Strategic Planning and Policy Development	2.04
	Systems Requirements Planning	2.01
Other	Customer Service and Technical Support	1.98
	Systems Requirements Planning	1.94

Participants in the 2210 Information Technology Management occupational series reported the highest average proficiency rating in the **Customer Service and Technical Support** Specialty Area. Participants in six occupational series reported high average proficiency ratings in the **Systems Requirements Planning** Specialty Area. Participants in five occupational series reported high average proficiency ratings in the **Customer Service and Technical Support** Specialty Area. *Appendix C - Table 31 displays the full listing of average proficiency ratings by occupational series.*

Average Proficiency (Advanced/Expert) - Occupational Series

Key Findings - Advanced/Expert Proficiency (by Occupational Series)
• Participants in the 2210 Information Technology Management series have the highest Advanced/Expert proficiency ratings across Specialty Areas. • Five occupational series had high average Advanced/Expert proficiency ratings in the **Systems Requirements Planning** Specialty Area.

The occupational series with Advanced (level 3) or Expert (level 4) proficiency in the cybersecurity Specialty Areas was also reported for the occupational series with the most participants. For each occupational series, the two Specialty Areas with the most participants with Advanced or Expert proficiency are displayed in Table 14.

Table 14: Participants with Advanced/Expert Proficiency - Occupational Series

Occupational Series	Specialty Area (Top Two)	Advanced/Expert Current Proficiency
2210	Customer Service and Technical Support	58.85%
	Systems Requirements Planning	50.02%
1801	Investigation	12.27%
	Education and Training	8.29%
0301	Data Administration	11.75%
	Knowledge Management	11.71%
0343	Knowledge Management	12.93%
	Data Administration	12.25%
1101	Customer Service and Technical Support	5.98%
	Data Administration	5.89%

Occupational Series	Specialty Area (Top Two)	Advanced/Expert Current Proficiency
1811	Investigation	38.63%
	Digital Forensics	17.90%
0855	Test and Evaluation	30.46%
	Systems Requirements Planning	30.09%
1550	Systems Requirements Planning	41.47%
	Systems Development	39.08%
0340	Strategic Planning and Policy Development	16.24%
	Systems Requirements Planning	14.59%
Other	Customer Service and Technical Support	14.12%
	Systems Requirements Planning	11.89%

Participants in the 2210 Information Technology Management occupational series have high percentages of Advanced or Expert proficiency for each of the cybersecurity Specialty Areas. The **Systems Requirements Planning** Specialty Area had either the highest or second highest percentage of Advanced or Expert proficiency for five occupational series. *Appendix C - Table 32 displays the full listing of the percentages of participants (by occupational series) with either Advanced or Expert proficiency*.

Average Proficiency (Meets/Exceeds Optimal) - Occupational Series

Key Findings - Meets/Exceeds Optimal Proficiency (by Occupational Series)
• 0340 Program Management series had highest percentage of participants meeting/exceeding optimal proficiency for **All Source Intelligence** (80.25%). • Five occupational series accounted for high percentages of meets/exceeds optimal proficiency for **Customer Services and Technical Support**.

The participants (by occupational series) that meet or exceed optimal proficiency for the Specialty Areas were also analyzed for the 10 most populous series. For each of the occupational series, the two Specialty Areas with the highest percentages of participants meeting or exceeding optimal proficiency are displayed in Table 15.

Table 15: Participants that Meet/Exceed Optimal Proficiency - Occupational Series

Occupational Series	Specialty Area (Top Two)	Meets/Exceeds Optimal Proficiency
2210	Customer Service and Technical Support	76.56%
	Systems Requirements Planning	66.28%
1801	Network Services	69.07%
	Systems Development	67.93%

Occupational Series	Specialty Area (Top Two)	Meets/Exceeds Optimal Proficiency
0301	Education and Training	74.25%
	Customer Service and Technical Support	71.88%
0343	Computer Network Defense (CND) Analysis	74.63%
	Collection Operations	73.33%
1101	All Source Intelligence	77.19%
	Vulnerability Assessment and Management	76.77%
1811	Customer Service and Technical Support	69.05%
	Systems Development	69.01%
0855	Customer Service and Technical Support	70.75%
	Security Program Management (Chief Information Security Officer [CISO])	68.57%
1550	Customer Service and Technical Support	73.18%
	Knowledge Management	65.68%
0340	All Source Intelligence	80.25%
	Threat Analysis	79.17%
Other	Education and Training	74.77%
	Security Program Management (Chief Information Security Officer [CISO])	71.16%

The 0340 Program Management occupational series had the highest percentage of participants meeting or exceeding optimal proficiency for the **All Source Intelligence** Specialty Area. The **Customer Services and Technical Support** Specialty Area had the highest or second highest number of participants meeting or exceeding optimal proficiency across five occupational series. *Appendix C – Table 33 displays the full listing of the percentages of participants (by occupational series) that meet or exceed optimal proficiency.*

Average Proficiency - 2210 Series Parenthetical Titles

Key Findings - Average Proficiency
• The Systems Administration parenthetical title accounted for the highest average proficiency rating for **Customer Service and Technical Support** (3.16). • Nine parentheticals titles accounted for high average proficiency ratings for **Customer Service and Technical Support.** • Five parentheticals titles accounted for high average proficiency ratings for the **Systems Requirements Planning** Specialty Area.

Since the majority of the assessment participants belonged to the 2210 series, the average proficiency levels were also identified for the 2210 series parenthetical titles. For each of

the parenthetical titles, the two Specialty Areas with the highest levels of proficiency are displayed in Table 16.

Table 16: Average Proficiency Ratings by 2210 Series Parenthetical Titles

2210 Series – Parenthetical Titles	Specialty Area (Top Two)	Average Proficiency Rating
Applications Software	Systems Requirements Planning	2.70
	Systems Development	2.68
Customer Support	Customer Service and Technical Support	3.11
	System Administration	2.41
Data Management	Data Administration	2.91
	Customer Service and Technical Support	2.88
Enterprise Architecture	Systems Requirements Planning	2.86
	Customer Service and Technical Support	2.64
Internet	Customer Service and Technical Support	2.69
	System Administration	2.40
Network Services	Customer Service and Technical Support	3.03
	Network Services	2.79
Operating Systems	Customer Service and Technical Support	3.03
	Systems Requirements Planning	2.77
Policy and Planning	Systems Requirements Planning	2.69
	Customer Service and Technical Support	2.66
Security	Information Assurance (IA) Compliance	3.07
	Information Systems Security Operations (Information Systems Security Officer [ISSO])	2.92
Systems Administration	Customer Service and Technical Support	3.16
	System Administration	3.03
Systems Analysis	Customer Service and Technical Support	2.66
	Systems Requirements Planning	2.66

Participants in the Systems Administration parenthetical title reported the highest average proficiency rating in the **Customer Service and Technical Support** Specialty Area. **Customer Service and Technical Support** had either the highest or second highest average proficiency for nine parenthetical titles followed by **Systems Requirements Planning** with five. *Appendix C – Table 34 displays the full listing of average proficiency ratings for the 2210 series parenthetical titles.*

Average Proficiency (Advanced/Expert) – 2210 Series Parenthetical Titles

Key Findings - Advanced/Expert Proficiency (2210 Series Parenthetical Titles)
• Participants in Systems Administration parenthetical title reported the highest percentage of Advanced/Expert proficiency in the **Customer Service and Technical Support Specialty Area** (77.99%). • Nine parenthetical titles reported high percentages of participants with Advanced/Expert proficiency in the **Customer Service and Technical Support Specialty Area**.

The participants in the 2210 series parenthetical titles with self-assessed Advanced (level 3) or Expert (level 4) proficiency, in cybersecurity Specialty Areas, was also captured. For each parenthetical title, the two Specialty Areas with the highest percentages of participants with Advanced or Expert proficiency are displayed in Table 17.

Table 17: Participants with Advanced/Expert Proficiency - 2210 Series Parenthetical Titles

2210 Series – Parenthetical Titles	Specialty Area (Top Two)	Advanced/Expert Proficiency
Applications Software	Systems Requirements Planning	56.85%
	Systems Development	53.97%
Customer Support	Customer Service and Technical Support	72.95%
	System Administration	38.92%
Data Management	Customer Service and Technical Support	65.62%
	Data Administration	64.98%
Enterprise Architecture	Systems Requirements Planning	61.18%
	Customer Service and Technical Support	48.68%
Internet	Customer Service and Technical Support	48.15%
	Systems Requirements Planning	38.27%
	Knowledge Management	38.27%
Network Services	Customer Service and Technical Support	70.08%
	Network Services	59.85%
Operating Systems	Customer Service and Technical Support	66.67%
	Systems Requirements Planning	51.43%
Policy and Planning	Systems Requirements Planning	53.69%
	Customer Service and Technical Support	48.05%
Security	Information Assurance (IA) Compliance	72.36%
	Vulnerability Assessment and Management	63.74%
Systems Administration	Customer Service and Technical Support	77.99%
	System Administration	70.91%
Systems Analysis	Systems Requirements Planning	54.74%
	Customer Service and Technical Support	50.16%

The Systems Administration parenthetical title had the highest percentage of Advanced or Expert proficiency for the **Customer Service and Technical Support** Specialty Area. Nine 2210 primary parenthetical titles indicated **Customer Service and Technical Support** as a Specialty Area that accounted for high percentages of Advanced or Expert proficiency. *Appendix C – Table 35 displays the full listing of the percentages of participants (by 2210 series parenthetical titles) with either Advanced/Expert proficiency.*

Average Proficiency (Meets/Exceeds Optimal Proficiency) – 2210 Series Parenthetical Titles

Key Findings - Meets/Exceeds Optimal Proficiency (2210 Parenthetical Titles)
• Ten parenthetical titles report high percentages meeting/exceeding optimal proficiency for **Customer Service and Technical Support**. • Enterprise Architecture parenthetical title had highest percentage meeting/exceeding proficiency for this Specialty Area (83.96%).

The participants in the 2210 series parenthetical titles that meet or exceed optimal proficiency, based on self-assessment, were also identified. For each parenthetical title, the two Specialty Areas with the highest percentages meeting or exceeding optimal proficiency are displayed in Table 18.

Table 18: Participants that Meet/Exceed Optimal Proficiency - 2210 Series Parenthetical Titles

2210 Series – Parenthetical Titles	Specialty Area (Top Two)	Meets/Exceeds Optimal Proficiency
Applications Software	Customer Service and Technical Support	77.30%
	Systems Requirements Planning	67.54%
Customer Support	Customer Service and Technical Support	76.67%
	Information Systems Security Operations (Information Systems Security Officer [ISSO])	69.05%
Data Management	Customer Service and Technical Support	75.63%
	System Administration	71.82%
Enterprise Architecture	Customer Service and Technical Support	83.96%
	System Administration	78.28%
Internet	Education and Training	76.67%
	Legal Advice and Advocacy	73.91%
Network Services	Customer Service and Technical Support	76.27%
	Knowledge Management	67.13%
Operating Systems	Customer Service and Technical Support	78.67%
	Education and Training	70.21%

2210 Series – Parenthetical Titles	Specialty Area (Top Two)	Meets/Exceeds Optimal Proficiency
Policy and Planning	Customer Service and Technical Support	76.65%
	Systems Development	69.71%
Security	Customer Service and Technical Support	75.94%
	Information Systems Security Operations (Information Systems Security Officer [ISSO])	68.13%
Systems Administration	Customer Service and Technical Support	77.23%
	System Administration	68.35%
Systems Analysis	Customer Service and Technical Support	75.35%
	Systems Requirements Planning	67.60%

The Enterprise Architecture parenthetical title had the highest percentage of participants meeting or exceeding optimal proficiency for the **Customer Service and Technical Support** Specialty Area. Ten 2210 parenthetical titles indicated **Customer Service and Technical Support** as the Specialty Area accounting for the highest percentage of participants meeting or exceeding optimal proficiency. *Appendix C – Table 36 displays the full listing of the percentages of participants (by 2210 series parenthetical titles) that meet or exceed optimal proficiency.*

4.3 Training Needs

The ITWAC participants indicated the Specialty Areas where they believe additional training could benefit them in their current role. Consistent with the previous sections, the training needs of the participants were first analyzed for the total assessment population, then by participant pay grade, occupational series, and 2210 parenthetical titles.

Training Needs - Total Assessment Population

Key Findings
• 26.83% of the assessment population indicated a training need in **Information Assurance (IA) Compliance**. • Participants also indicated strong need for training in **Vulnerability Assessment and Management** and **Knowledge Management.**

A high percentage of the ITWAC population indicated that it would be beneficial to have training in the **Information Assurance (IA) Compliance** followed by **Vulnerability Assessment and Management** and **Knowledge Management**. It could be assumed that a low proficiency level for a Specialty Area would indicate a higher need for training; however, in the case of the ITWAC data, this is not true.

Several Specialty Areas with high levels of proficiency also have high percentages of the population indicating their need for training. For example, the assessment population reported an average proficiency rating of 2.39 for **Customer Service and Technical**

Support and 73.90% of the population meets/exceeds optimal proficiency in this area. However, 12.79% of the population also indicated training in this Specialty Area would be beneficial for their current responsibilities.

A reason for this finding could be that participants desire additional training to become more proficient in a Specialty Area. It may also be that these Specialty Areas are rapidly changing and new developments require the need continually keep up training. *Appendix C – Table 25 displays the training needs of the total assessment population.*

Training Needs - Pay Grade

Key Findings
• Participants from GS 4 level and below indicated the highest need for training in **Information Assurance (IA) Compliance** (29.27%). • Participants from five pay grades indicated a high need for training in **Information Assurance (IA) Compliance.** • Senior leadership indicated the highest need for training in **Strategic Planning and Policy Development**.

For each pay grade, the two Specialty Areas with the highest percentage of participants indicating training needs are displayed in Table 19.

Table 19: Training Needs by Pay Grade

Pay Grade	Specialty Area (Top Two)	Training Needs (%)
GS 4 and below	Information Assurance (IA) Compliance	29.27%
	Customer Service and Technical Support	26.83%
GS 5-10	Information Assurance (IA) Compliance	21.74%
	Education and Training	20.38%
GS 11-13	Information Assurance (IA) Compliance	28.64%
	Vulnerability Assessment and Management	20.74%
GS 14-15	Information Assurance (IA) Compliance	25.87%
	Vulnerability Assessment and Management	20.80%
SES	Strategic Planning and Policy Development	23.96%
	Knowledge Management	21.35%
SL/ST	Strategic Planning and Policy Development	25.64%
	Knowledge Management	23.08%
	Threat Analysis	23.08%
	Systems Security Architecture	23.08%
Other	Information Assurance (IA) Compliance	22.30%
	Vulnerability Assessment and Management	21.23%

The GS 4 and below pay grade indicated the highest need for training in **Information Assurance (IA) Compliance**. There is a training need across pay grades in **Information Assurance (IA) Compliance**. Amongst the senior leadership, there is a training need in **Strategic Planning and Policy Development**. *Appendix C – Table 37 displays the full listing of training needs percentages by pay grade.*

Training Needs - Occupational Series

Key Findings
• Participants in the1811 - Criminal Investigation occupational series indicated a strong need for training in the **Investigation** Specialty Area (65.84%). • Participants in four occupational series indicated a need for training in **Information Assurance (IA) Compliance** and **Knowledge Management**.

For training needs, the participants were also broken down by the 10 occupational series with the most participants. *Refer to Appendix C – Table 24 for the full title of each occupational series.* For each occupational series, the two Specialty Areas with the highest percentage indicating a training need are displayed in Table 20.

Table 20: Training Needs by Occupational Series

Occupational Series	Specialty Area (Top Two)	Training Needs (%)
2210	Information Assurance (IA) Compliance	44.65%
	Vulnerability Assessment and Management	30.28%
1801	Investigation	34.62%
	Threat Analysis	23.09%
0301	Data Administration	22.76%
	Knowledge Management	22.63%
0343	Knowledge Management	26.15%
	Data Administration	20.80%
1101	Education and Training	17.17%
	Data Administration	13.89%
1811	Investigation	65.84%
	Digital Forensics	46.12%
0855	Information Assurance (IA) Compliance	36.94%
	Test and Evaluation	28.24%
1550	Information Assurance (IA) Compliance	38.91%
	Software Assurance and Security Engineering	34.13%
0340	Knowledge Management	22.82%
	Vulnerability Assessment and Management	21.18%
Other	Knowledge Management	17.44%
	Information Assurance (IA) Compliance	17.00%

The 1811 - Criminal Investigation occupational series accounted for the highest percentage of participants indicating a need for training in the **Investigation** Specialty Area. Four occupational series had either the highest or second highest need for training in **Information Assurance (IA) Compliance** and **Knowledge Management**. *Appendix C – Table 38 displays the full listing of participant training needs by occupational series.*

Training Needs - Parenthetical Titles

Key Findings
• Participants in the Security parenthetical title indicated strongest need for training in the **Information Assurance (IA) Compliance** Specialty Area (54.66%)**.** • Participants from 10 parenthetical titles indicated a need for training in **Information Assurance (IA) Compliance**.

The training needs were also captured for participants in the 2210 series parenthetical titles. For each parenthetical title, the two Specialty Areas with the highest percentage of participants indicating a training need are displayed in Table 21.

Table 21: Training Needs by 2210 Series Parenthetical Titles

2210 Series – Parenthetical Titles	Specialty Area	Training Needs (%)
Applications Software	Information Assurance (IA) Compliance	39.73%
	Software Assurance and Security Engineering	38.08%
Customer Support	Customer Service and Technical Support	49.94%
	Information Assurance (IA) Compliance	41.37%
Data Management	Data Administration	54.57%
	Information Assurance (IA) Compliance	41.32%
Enterprise Architecture	Systems Security Architecture	50.00%
	Information Assurance (IA) Compliance	45.39%
Internet	Information Assurance (IA) Compliance	39.51%
	Knowledge Management	33.33%
Network Services	Network Services	51.92%
	Information Assurance (IA) Compliance	43.22%
Operating Systems	Information Assurance (IA) Compliance	41.90%
	Systems Security Architecture	32.38%
Policy and Planning	Information Assurance (IA) Compliance	47.32%
	Strategic Planning and Policy Development	36.18%
Security	Information Assurance (IA) Compliance	54.66%
	Vulnerability Assessment and Management	45.42%
Systems Administration	System Administration	53.93%
	Systems Security Architecture	45.56%

2210 Series – Parenthetical Titles	Specialty Area	Training Needs (%)
Systems Analysis	Information Assurance (IA) Compliance	41.67%
	Systems Requirements Planning	33.17%

The Security parenthetical title reported the highest percentage of participants indicating a need for training in the **Information Assurance (IA) Compliance** Specialty Area. The **Information Assurance (IA) Compliance** Specialty Area was a top training need for participants from 10 parenthetical titles. *Appendix C – Table 39 displays a full listing of participant training needs for the 2210 series parenthetical titles*.

5. Conclusion

This report seeks to summarize the current landscape of the federal cybersecurity civilian workforce. The workforce demographics (i.e., composition) and capabilities data can provide departments and agencies with a better understanding of the federal civilian cybersecurity workforce.

A broad implication of the findings is that the majority of the federal cybersecurity professional population is above the age of 40.

In addition, there are multiple occupational series that include cybersecurity professionals. Departments and agencies may be unaware that, while the 2210 series accounts for the largest portion, cybersecurity professionals are dispersed across other occupational series.

Finally, participants from several pay grades and 2210 series parenthetical titles indicated a need for training in **Information Assurance (IA) Compliance**. This might imply that more training is needed (for various target populations) in this particular Specialty Area.

The purpose of the ITWAC is to provide a current snapshot of the federal civilian IT workforce with cybersecurity duties and responsibilities. The data can serve as a starting point for examining critical skills, determining skill gaps, and identifying training to mitigate gaps. It can also illustrate the current workforce supply and provide an understanding of the cybersecurity workforce pipeline (e.g., the age of the workforce and the percentage eligible for retirement).

Federal departments and agencies can use the data to support strategic cybersecurity workforce development activities such as workforce planning and professional development. Activities such as these can ensure that the federal cybersecurity workforce is properly equipped to respond to and protect the United States from cyber threats and attacks.

We would like to thank the participating departments and agencies as well as all the participants who took the time to complete the ITWAC. The feedback provided is essential in shaping the future environment of the federal cybersecurity workforce.

Appendix A: Glossary of Terms and Acronyms

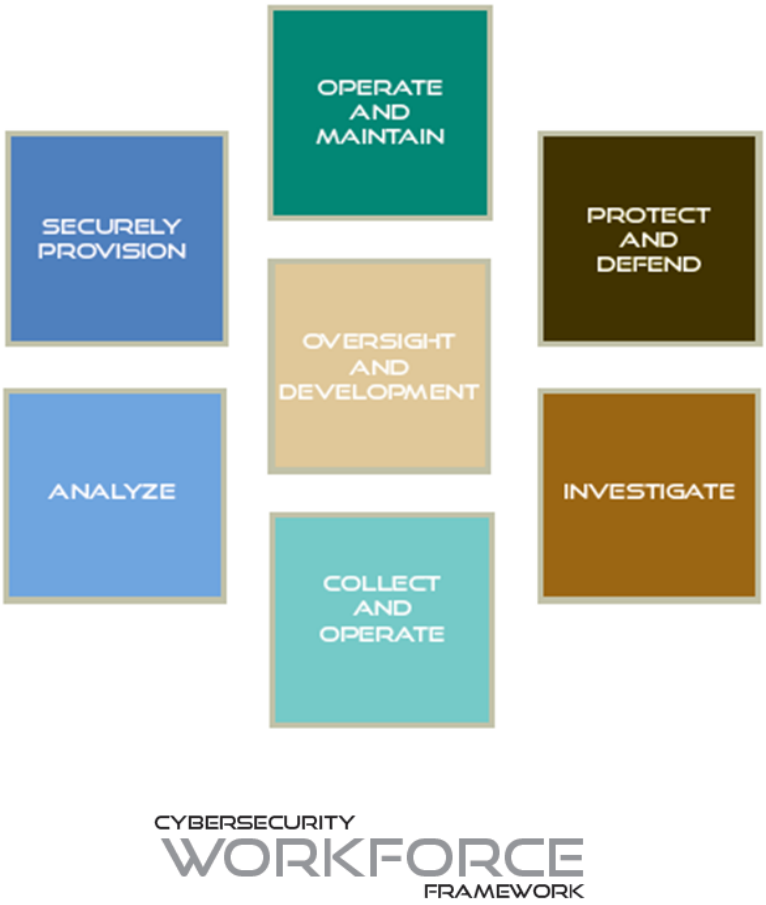
Table 22: Terms and Acronyms

Term	Definition
Competency	A measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual must display to successfully perform job duties and tasks.
Cybersecurity	The strategy, policy, and standards regarding the security of and operations in cyberspace; encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Cyberspace Policy Review)
Cybersecurity Pipeline	The people coming out of our K-20 system with the cybersecurity skills necessary to meet the nation's cybersecurity needs as well as those who transition into professional cybersecurity roles.
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people. (Cyberspace Policy Review)
ITWAC	Information Technology Workforce Assessment for Cybersecurity
ITWCA	Information Technology Capability Assessment last conducted in 2011 by the Federal Chief Information Officers Council.
National Cybersecurity Workforce Framework (the Framework)	Provides a baseline of knowledge, skills, and abilities for professionals across the diverse array of cybersecurity disciplines and a foundation for the education and training necessary to excel in these careers; facilitates the identification of training needs and guides the design of a professional development program.
Proficiency	The degree to which an individual is expected to demonstrate a particular competency (specialty area) within a job role. Participants were asked to self-report their current levels of proficiency, in relation to the Specialty Areas, as well as the levels of proficiency required for someone in their role (optimal proficiency).
SLTT	Federal acronym for State, Local, Tribal, and Territorial, which refers to non-Federal Governments.
Specialty Area	High level cybersecurity functions found within the National Cybersecurity Workforce Framework.

Appendix B: The Framework

The following graphic is a visual representation of the seven categories of the National Cybersecurity Workforce Framework.

Figure 6: The Framework



Appendix C: Additional Data Tables and Figures

The following table displays the 52 federal departments and agencies that participated in the ITWAC.

Table 23: Agency Participation

Department/Agency	
Access Board	Executive Office of the President
African Development Foundation	Farm Credit Administration
Commission of Fine Arts	Farm Credit System Insurance Corporation
Commission on the Prevention of Weapons of Mass Destruction Proliferation	Federal Communications Commission
Corporation for National and Community Service	Federal Deposit Insurance Corporation
Court Services and Offender Supervision Agency for the District of Columbia	Federal Election Commission
Defense Nuclear Facilities Safety Board	Federal Housing Finance Agency
Delta Regional Authority	Federal Reserve System
Department of Agriculture	Federal Trade Commission
Department of the Air Force	General Services Administration
Department of the Army	Government Printing Office
Department of Commerce	Inter-American Foundation
Department of Defense	International Broadcasting Bureau
Department of Education	National Aeronautics and Space Administration
Department of Energy	National Commission on Libraries and Information Science
Department of Health and Human Services	National Labor Relations Board
Department of Homeland Security	National Science Foundation
Department of Housing and Urban Development	Nuclear Regulatory Commission
Department of the Interior	Office of Personnel Management
Department of Justice	Peace Corps
Department of Labor	Postal Regulatory Commission
Department of the Navy	Postal Service
Department of Transportation	Selective Service System
Department of the Treasury	Small Business Administration
Environmental Protection Agency	Social Security Administration
Equal Employment Opportunity Commission	U.S. Agency for International Development

The table below displays the occupational series that were listed as response options in the ITWAC.

Table 24: Occupational Series Options

Occupational Series	
0080 - Security Administration Series	1410 - Librarian Series
0132 - Intelligence Series	1411 - Library Technician Series
0301 - Miscellaneous Administration and Program	1412 - Technical Information Services Series
0332 - Computer Operation	1420 - Archivist Series
0334 - Computer Specialist	1421 - Archives Technician Series
0335 - Computer Clerk and Assistant	1515 - Operations Research
0340 - Program Management	1540 - Cryptography Series
0343 - Management and Program Analysis	1541 - Cryptanalysis Series
0390 - Telecommunications Processing Series	1550 - Computer Science Series
0391 - Telecommunications Series	1701 - General Education and Training Series
0394 - Communications Clerical Series	1801 - General Inspection, Investigation, Enforcement, and Compliance
0501 - Financial Administration and Program	1805 - Investigative Analysis
0510 – Accounting	1810 - General Investigation
0511 – Auditing	1811 - Criminal Investigation
0801 - General Engineering and Architecture	2210 - Information Technology Management
0850 - Electrical Engineering	2880 - Foreign Service
0854 - Computer Engineering	2882 - Foreign Service
0855 - Electronics Engineering	2884 - Foreign Service
0856 - Electronics Technical	Other - (i.e., other occupational series not listed in response options)
1101 - General Business and Industry Series	

The following figures display additional demographic data of the assessment participants.

Figure 7: Participant Gender

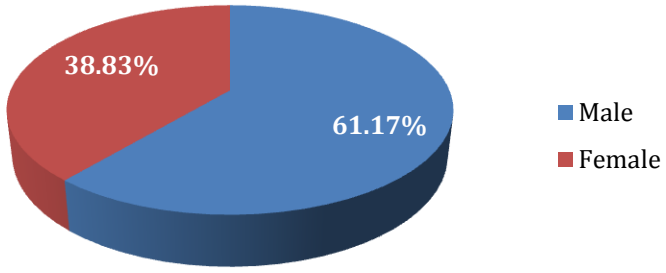


Figure 8: Participant Ethnicity

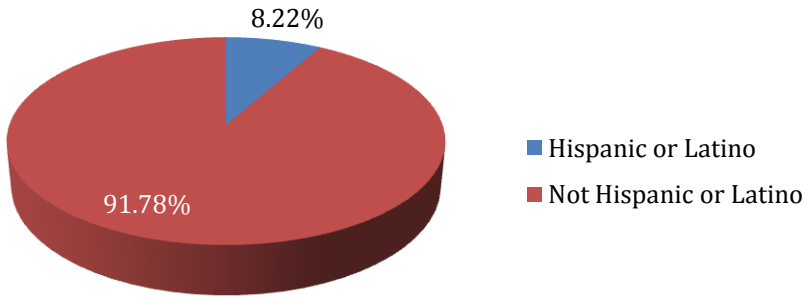


Figure 9: Participant Race/National Origin

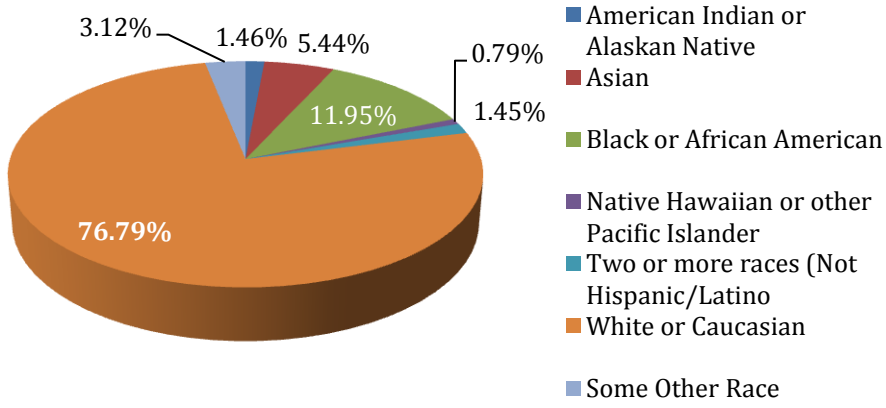


Figure 10: Participant Disability Status

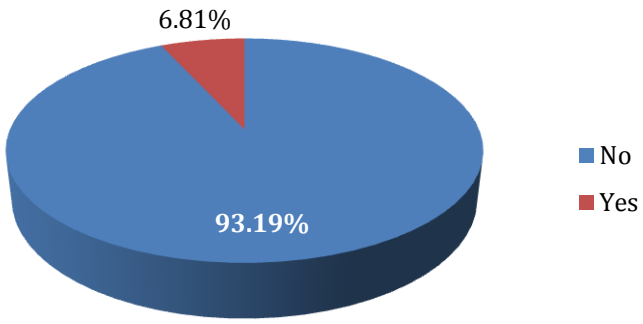


Figure 11: Participant Veteran Status

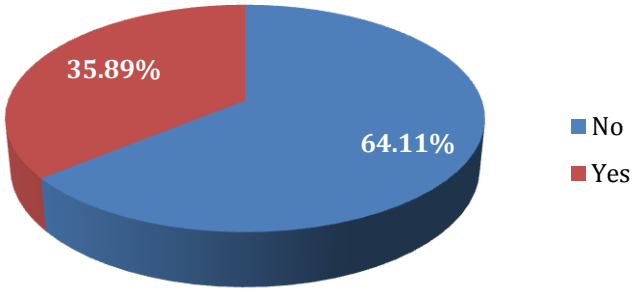


Table 25: Total Assessment Population Findings

Specialty Area	Average Time Spent in Specialty Area (%)	Average Proficiency Rating w/Level 0	Average Proficiency Rating w/o Level 0	Meets or Exceeds Optimal Proficiency (%)	Advanced/Expert Proficiency (%)	Training Needs (%)
Information Assurance (IA) Compliance	3.91%	1.24	2.02	58.90%	18.84%	26.83%
Software Assurance and Security Engineering	1.32%	0.76	1.87	60.41%	10.34%	10.93%
Systems Security Architecture	0.74%	0.90	1.96	59.05%	13.51%	14.72%
Technology Research and Development	1.53%	1.01	2.06	63.30%	16.20%	9.71%
Systems Requirements Planning	3.27%	1.31	2.28	66.29%	24.26%	14.17%
Test and Evaluation	2.69%	1.15	2.17	64.12%	20.05%	13.86%
Systems Development	2.28%	1.04	2.13	66.39%	17.83%	12.49%
Data Administration	3.25%	1.13	1.92	64.84%	15.97%	16.61%
Knowledge Management	2.53%	1.19	1.99	65.35%	17.87%	18.22%
Customer Service and Technical Support	6.40%	1.37	2.39	73.90%	26.82%	12.79%
Network Services	1.26%	0.85	1.96	61.82%	12.38%	12.91%
System Administration	2.21%	0.95	2.14	65.14%	16.33%	14.56%
Systems Security Analysis	0.55%	0.9	2.04	63.28%	14.25%	11.60%
Computer Network Defense (CND) Analysis	0.40%	0.78	1.81	61.68%	9.98%	8.98%
Incident Response	1.19%	0.93	1.94	63.46%	13.87%	15.75%
Computer Network Defense (CND) Infrastructure Support	0.23%	0.66	1.84	60.36%	8.75%	8.30%

Specialty Area	Average Time Spent in Specialty Area (%)	Average Proficiency Rating w/Level 0	Average Proficiency Rating w/o Level 0	Meets or Exceeds Optimal Proficiency (%)	Advanced/Expert Proficiency (%)	Training Needs (%)
Vulnerability Assessment and Management	1.05%	0.85	1.97	62.19%	13.03%	19.81%
Investigation	2.42%	0.7	1.88	58.87%	9.87%	15.50%
Digital Forensics	0.52%	0.59	1.72	56.61%	6.79%	13.08%
Collection Operations	0.55%	0.59	1.75	62.06%	7.23%	7.48%
Cyber Operations Planning	0.18%	0.51	1.75	59.05%	6.14%	7.65%
Cyber Operations	0.18%	0.48	1.73	58.54%	5.67%	9.64%
Threat Analysis	0.40%	0.51	1.72	57.72%	6.03%	15.60%
Exploitation Analysis	0.34%	0.58	1.77	58.13%	7.29%	8.12%
All Source Intelligence	0.39%	0.52	1.75	57.74%	6.35%	8.20%
Targets	0.31%	0.52	1.73	59.60%	6.04%	5.95%
Legal Advice and Advocacy	0.41%	0.52	1.77	61.19%	6.53%	6.97%
Strategic Planning and Policy Development	2.04%	0.84	1.96	62.90%	12.56%	11.63%
Education and Training	1.95%	0.91	2.01	66.57%	14.33%	16.69%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	1.09%	0.72	2.01	64.02%	11.27%	11.75%
Security Program Management (Chief Information Security Officer [CISO])	0.60%	0.62	1.9	62.08%	8.85%	8.28%
All Other Work	53.81%	NA	NA	NA	NA	NA

Table 26: Time Spent in Specialty Areas by Pay Grade

Specialty Area	Pay Grades						
	GS 4 and Below	GS 5-10	GS 11-13	GS 14-15	SES	SL/ST	Other
Information Assurance (IA) Compliance	5.37%	3.06%	4.16%	3.78%	1.07%	3.49%	4.02%
Software Assurance and Security Engineering	0.17%	0.69%	1.73%	0.67%	0.38%	0.31%	1.05%
Systems Security Architecture	1.49%	0.28%	0.73%	1.08%	0.47%	1.72%	0.50%
Technology Research and Development	0.73%	0.68%	1.47%	2.20%	1.00%	6.28%	1.34%
Systems Requirements Planning	1.71%	1.43%	3.46%	4.08%	1.97%	2.90%	1.90%
Test and Evaluation	5.02%	1.30%	3.05%	2.47%	0.62%	2.51%	3.06%
Systems Development	0.93%	0.69%	2.42%	2.94%	0.70%	3.33%	1.81%
Data Administration	0.98%	4.42%	3.58%	1.88%	0.97%	0.77%	2.60%
Knowledge Management	2.07%	2.33%	2.54%	2.79%	1.85%	4.38%	1.47%
Customer Service and Technical Support	6.07%	7.98%	7.31%	3.40%	2.26%	1.21%	4.62%
Network Services	0.88%	0.89%	1.56%	0.67%	0.32%	0.00%	1.21%
System Administration	6.51%	1.81%	2.78%	0.99%	0.34%	0.00%	1.68%
Systems Security Analysis	0.61%	0.25%	0.61%	0.57%	0.27%	0.00%	0.50%
Computer Network Defense (CND) Analysis	0.98%	0.44%	0.41%	0.40%	0.04%	0.26%	0.29%
Incident Response	6.56%	0.77%	1.20%	1.27%	1.60%	0.44%	1.85%
Computer Network Defense (CND) Infrastructure Support	0.07%	0.13%	0.25%	0.25%	0.36%	0.00%	0.11%
Vulnerability Assessment and Management	0.93%	0.44%	1.11%	1.27%	0.90%	0.46%	0.97%
Investigation	0.56%	2.16%	2.61%	2.08%	3.32%	0.56%	1.97%

Specialty Area	Pay Grades						
	GS 4 and Below	GS 5-10	GS 11-13	GS 14-15	SES	SL/ST	Other
Digital Forensics	0.15%	0.31%	0.61%	0.44%	0.31%	0.10%	0.27%
Collection Operations	0.63%	0.69%	0.58%	0.43%	0.30%	0.00%	0.41%
Cyber Operations Planning	0.00%	0.08%	0.16%	0.31%	0.25%	0.69%	0.06%
Cyber Operations	0.78%	0.12%	0.19%	0.20%	0.15%	0.00%	0.06%
Threat Analysis	0.20%	0.26%	0.39%	0.51%	0.62%	0.74%	0.26%
Exploitation Analysis	0.71%	0.21%	0.36%	0.36%	0.14%	0.26%	0.44%
All Source Intelligence	0.17%	0.22%	0.39%	0.51%	0.55%	0.38%	0.24%
Targets	0.37%	0.29%	0.32%	0.31%	0.36%	0.00%	0.21%
Legal Advice and Advocacy	0.00%	0.21%	0.37%	0.65%	0.63%	1.03%	0.14%
Strategic Planning and Policy Development	1.41%	0.54%	1.52%	4.35%	6.20%	8.97%	0.62%
Education and Training	2.85%	1.58%	2.00%	2.09%	1.86%	1.69%	1.61%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	0.20%	0.53%	1.16%	1.37%	0.33%	0.95%	0.54%
Security Program Management (Chief Information Security Officer [CISO])	0.12%	0.14%	0.45%	1.31%	1.36%	2.49%	0.24%
All Other Work	50.77%	65.07%	50.52%	54.37%	68.50%	54.08%	63.95%

Table 27: Time Spent in Specialty Areas by Occupational Series

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Information Assurance (IA) Compliance	1.32%	0.83%	1.15%	3.18%	0.71%	6.27%	1.07%	0.62%	8.51%	2.83%
Software Assurance and Security Engineering	0.20%	0.17%	0.24%	1.67%	0.11%	7.96%	0.06%	0.02%	2.52%	0.88%
Systems Security Architecture	0.14%	0.39%	0.29%	1.19%	0.06%	2.09%	0.07%	0.03%	1.53%	0.36%
Technology Research and Development	0.42%	0.60%	0.56%	6.35%	0.15%	6.23%	0.16%	0.17%	2.20%	0.70%
Systems Requirements Planning	1.21%	2.08%	2.10%	4.95%	0.64%	5.13%	0.41%	0.23%	6.12%	2.15%
Test and Evaluation	0.67%	1.29%	1.06%	8.45%	0.55%	8.58%	0.38%	0.27%	4.39%	1.64%
Systems Development	0.54%	1.52%	1.01%	5.31%	0.24%	8.98%	0.15%	0.06%	3.95%	1.41%
Data Administration	5.11%	1.98%	4.13%	1.61%	2.03%	2.94%	1.87%	0.68%	4.05%	3.48%
Knowledge Management	3.31%	2.39%	4.02%	1.58%	1.28%	2.72%	1.27%	0.45%	3.23%	2.42%
Customer Service and Technical Support	2.65%	2.06%	2.30%	2.95%	2.52%	3.65%	0.82%	0.20%	14.40%	4.12%
Network Services	0.16%	0.30%	0.03%	1.15%	0.14%	1.38%	0.07%	0.08%	2.99%	0.66%
System Administration	0.29%	0.38%	0.32%	1.34%	0.28%	3.22%	0.16%	0.09%	5.62%	0.97%
Systems Security Analysis	0.11%	0.19%	0.08%	0.39%	0.07%	0.90%	0.09%	0.06%	1.30%	0.23%
Computer Network Defense (CND) Analysis	0.20%	0.12%	0.11%	0.14%	0.15%	0.57%	0.38%	0.29%	0.73%	0.42%
Incident Response	0.92%	1.00%	0.63%	0.20%	0.39%	0.62%	1.63%	0.75%	1.82%	1.34%
Computer Network Defense (CND) Infrastructure Support	0.04%	0.03%	0.01%	0.20%	0.04%	0.35%	0.04%	0.08%	0.55%	0.08%
Vulnerability Assessment and Management	0.31%	1.10%	0.30%	0.57%	0.23%	1.70%	0.59%	0.59%	2.21%	0.41%
Investigation	0.35%	0.61%	0.34%	0.09%	0.40%	0.35%	5.84%	26.48%	0.38%	0.79%
Digital Forensics	0.08%	0.11%	0.09%	0.05%	0.06%	0.39%	0.81%	4.72%	0.30%	0.11%
Collection Operations	0.44%	0.77%	0.54%	0.18%	0.61%	0.18%	0.80%	1.31%	0.43%	0.55%

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Cyber Operations Planning	0.07%	0.09%	0.13%	0.08%	0.04%	0.31%	0.06%	0.31%	0.34%	0.06%
Cyber Operations	0.12%	0.14%	0.04%	0.05%	0.02%	0.12%	0.28%	0.76%	0.18%	0.09%
Threat Analysis	0.18%	0.31%	0.18%	0.27%	0.06%	0.30%	0.62%	0.91%	0.44%	0.20%
Exploitation Analysis	0.11%	0.10%	0.31%	0.15%	0.08%	0.33%	0.48%	0.50%	0.43%	0.19%
All Source Intelligence	0.19%	0.30%	0.18%	0.16%	0.05%	0.17%	0.78%	1.00%	0.21%	0.10%
Targets	0.13%	0.40%	0.22%	0.09%	0.23%	0.06%	0.84%	0.91%	0.14%	0.26%
Legal Advice and Advocacy	0.43%	0.55%	0.51%	0.10%	0.41%	0.20%	0.65%	0.24%	0.49%	0.22%
Strategic Planning and Policy Development	1.88%	4.51%	3.51%	0.83%	0.40%	1.89%	0.66%	0.45%	3.42%	1.11%
Education and Training	1.84%	1.89%	2.23%	0.64%	1.21%	1.09%	1.83%	1.07%	2.69%	1.55%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	0.24%	0.47%	0.35%	0.35%	0.11%	0.92%	0.10%	0.04%	2.85%	0.47%
Security Program Management (Chief Information Security Officer [CISO])	0.17%	0.57%	0.38%	0.18%	0.14%	0.47%	0.16%	0.08%	1.39%	0.21%
All Other Work	76.17%	72.75%	72.65%	55.55%	86.59%	29.93%	76.87%	56.55%	20.19%	69.99%

Table 28: Time Spent in Specialty Areas is 100%

Occupational Series																			
0301		0340		0343		0855		1101		1550		1801		1811		2210		Other		Total
#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#
253	10.93	50	11.76	216	12.31	240	22.22	74	6.23	212	36.18	300	11.16	265	24.20	3033	43.35	217	15.63	4,860

Table 29: Time Spent in Specialty Areas by 2210 Series Parenthetical Titles

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Information Assurance (IA) Compliance	3.51%	3.95%	4.06%	4.07%	2.35%	4.98%	4.87%	7.34%	23.73%	6.37%	4.65%
Software Assurance and Security Engineering	12.85%	0.52%	4.00%	0.62%	5.70%	0.50%	1.46%	0.41%	0.60%	1.10%	1.73%
Systems Security Architecture	1.54%	0.37%	1.07%	5.37%	0.99%	1.62%	2.67%	1.52%	2.17%	1.22%	1.85%
Technology Research and Development	2.89%	1.03%	2.50%	5.69%	4.12%	2.39%	1.96%	2.36%	1.65%	1.73%	3.10%
Systems Requirements Planning	8.67%	4.14%	4.46%	9.33%	5.51%	4.93%	5.96%	8.36%	2.70%	3.71%	12.76%
Test and Evaluation	11.72%	2.10%	3.06%	2.96%	2.57%	2.45%	5.63%	2.05%	2.88%	2.91%	8.13%
Systems Development	14.10%	0.97%	5.57%	3.59%	3.84%	2.15%	2.43%	1.96%	1.16%	1.82%	7.13%
Data Administration	4.98%	2.81%	26.50%	2.82%	4.81%	2.36%	2.86%	1.68%	0.86%	4.92%	3.56%
Knowledge Management	2.65%	2.89%	5.33%	5.09%	5.09%	2.98%	2.71%	4.85%	1.64%	3.21%	3.84%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Customer Service and Technical Support	8.73%	42.53%	10.64%	5.87%	11.57%	16.30%	16.33%	7.09%	4.96%	20.74%	9.77%
Network Services	0.23%	3.14%	0.50%	3.56%	1.01%	20.88%	1.88%	1.49%	1.34%	4.22%	1.46%
System Administration	1.77%	4.91%	4.07%	2.78%	4.44%	6.69%	13.56%	1.63%	2.19%	22.80%	3.41%
Systems Security Analysis	0.70%	0.53%	0.54%	1.12%	0.53%	1.26%	0.85%	0.68%	2.85%	2.08%	1.13%
Computer Network Defense (CND) Analysis	0.14%	0.35%	0.32%	0.33%	0.14%	1.06%	0.13%	0.37%	2.15%	0.55%	0.49%
Incident Response	0.62%	2.18%	0.99%	0.70%	0.59%	1.72%	2.00%	1.20%	3.76%	1.69%	1.40%
Computer Network Defense (CND) Infrastructure Support	0.13%	0.22%	0.18%	0.34%	0.20%	1.48%	0.25%	0.40%	1.29%	0.53%	0.39%
Vulnerability Assessment and Management	0.48%	0.74%	0.81%	1.32%	0.68%	1.89%	1.21%	1.43%	6.53%	2.03%	1.42%
Investigation	0.06%	0.25%	0.39%	0.40%	0.14%	0.35%	0.49%	0.33%	0.90%	0.34%	0.20%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Digital Forensics	0.07%	0.09%	0.21%	0.00%	0.32%	0.16%	0.01%	0.10%	0.89%	0.20%	0.14%
Collection Operations	0.25%	0.43%	0.54%	0.28%	0.38%	0.37%	0.61%	0.44%	0.61%	0.43%	0.37%
Cyber Operations Planning	0.05%	0.09%	0.14%	0.45%	0.10%	0.21%	0.10%	1.12%	0.77%	0.10%	0.14%
Cyber Operations	0.04%	0.08%	0.11%	0.00%	0.17%	0.15%	0.01%	0.16%	0.57%	0.11%	0.05%
Threat Analysis	0.16%	0.25%	0.19%	0.64%	0.51%	0.29%	0.15%	0.23%	1.23%	0.24%	0.37%
Exploitation Analysis	0.09%	0.14%	0.30%	0.20%	0.27%	0.43%	0.16%	0.21%	1.31%	0.29%	0.25%
All Source Intelligence	0.04%	0.09%	0.13%	0.18%	0.20%	0.10%	0.10%	0.11%	0.64%	0.08%	0.19%
Targets	0.06%	0.11%	0.09%	0.12%	0.10%	0.12%	0.10%	0.15%	0.27%	0.10%	0.20%
Legal Advice and Advocacy	0.09%	0.17%	0.11%	0.53%	0.77%	0.47%	0.01%	1.39%	0.85%	0.20%	0.32%
Strategic Planning and Policy Development	1.21%	1.01%	1.25%	5.59%	3.58%	1.95%	4.15%	12.57%	3.91%	0.94%	2.45%
Education and Training	1.17%	2.61%	2.14%	2.98%	2.75%	1.80%	3.40%	3.60%	4.19%	2.06%	2.11%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Information Systems Security Operations (Information Systems Security Officer [ISSO])	0.40%	0.95%	1.14%	1.30%	0.35%	1.30%	1.34%	2.26%	9.51%	1.96%	1.39%
Security Program Management (Chief Information Security Officer [CISO])	0.11%	0.29%	0.31%	1.24%	0.01%	0.45%	0.12%	1.19%	5.10%	0.49%	0.40%
All Other Work	20.49%	20.06%	18.35%	30.53%	36.21%	16.21%	22.49%	31.32%	6.79%	10.83%	25.20%

Table 30: Average Proficiency by Pay Grade

Specialty Area	Pay Grades						
	GS 4 and Below	GS 5-10	GS 11-13	GS 14-15	SES	SL/ST	Other
Information Assurance (IA) Compliance	2.00	1.81	2.02	2.08	1.98	2.73	1.93
Software Assurance and Security Engineering	1.61	1.65	1.90	1.89	1.79	2.06	1.84
Systems Security Architecture	1.71	1.68	1.96	2.07	1.90	2.74	1.86
Technology Research and Development	1.76	1.76	2.05	2.18	1.93	2.70	1.96
Systems Requirements Planning	2.11	1.91	2.28	2.43	2.11	2.88	2.11
Test and Evaluation	2.24	1.83	2.18	2.25	1.97	2.54	2.05
Systems Development	1.94	1.74	2.12	2.27	1.97	2.64	2.00
Data Administration	1.83	1.87	1.95	1.88	1.74	1.79	1.82
Knowledge Management	1.90	1.83	2.00	2.03	1.88	2.19	1.87
Customer Service and Technical Support	2.05	2.19	2.47	2.28	2.07	2.17	2.19
Network Services	1.75	1.81	1.98	1.95	2.02	2.17	1.92
System Administration	1.78	1.95	2.21	2.05	1.85	2.41	2.04
Systems Security Analysis	1.93	1.78	2.06	2.08	1.83	2.29	1.95
Computer Network Defense (CND) Analysis	1.40	1.64	1.83	1.85	1.69	1.83	1.76
Incident Response	1.56	1.74	1.95	2.01	1.89	2.16	1.88
Computer Network Defense (CND) Infrastructure Support	1.60	1.63	1.86	1.92	1.81	2.00	1.73
Vulnerability Assessment and Management	1.56	1.69	1.99	2.06	1.78	2.26	1.84
Investigation	1.45	1.80	1.87	1.95	1.95	2.00	1.77

Specialty Area	Pay Grades						
	GS 4 and Below	GS 5-10	GS 11-13	GS 14-15	SES	SL/ST	Other
Digital Forensics	1.63	1.67	1.73	1.74	1.58	1.76	1.65
Collection Operations	1.50	1.64	1.75	1.80	1.78	1.74	1.64
Cyber Operations Planning	2.00	1.64	1.73	1.85	1.87	1.94	1.73
Cyber Operations	1.63	1.67	1.71	1.79	1.81	2.00	1.60
Threat Analysis	1.44	1.63	1.70	1.80	1.96	1.88	1.67
Exploitation Analysis	1.29	1.63	1.75	1.87	1.88	1.93	1.64
All Source Intelligence	1.50	1.64	1.73	1.83	1.88	2.00	1.65
Targets	1.56	1.62	1.71	1.81	2.04	1.88	1.65
Legal Advice and Advocacy	1.50	1.69	1.73	1.89	1.87	1.81	1.69
Strategic Planning and Policy Development	1.50	1.65	1.87	2.19	2.29	2.74	1.77
Education and Training	1.88	1.75	2.00	2.15	1.95	2.43	1.94
Information Systems Security Operations (Information Systems Security Officer [ISSO])	1.42	1.73	2.00	2.15	1.80	2.55	1.93
Security Program Management (Chief Information Security Officer [CISO])	1.64	1.65	1.87	2.03	2.00	2.33	1.78

Table 31: Average Proficiency by Occupational Series

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Information Assurance (IA) Compliance	1.62	1.71	1.65	1.75	1.57	2.11	1.64	1.55	2.36	1.79
Software Assurance and Security Engineering	1.58	1.71	1.53	1.73	1.56	2.16	1.63	1.53	1.99	1.78
Systems Security Architecture	1.61	1.76	1.57	1.77	1.56	2.01	1.61	1.61	2.16	1.77
Technology Research and Development	1.72	1.75	1.65	2.13	1.55	2.22	1.65	1.61	2.24	1.85
Systems Requirements Planning	1.87	2.01	1.85	2.20	1.59	2.42	1.75	1.67	2.59	1.94
Test and Evaluation	1.75	1.89	1.76	2.21	1.64	2.30	1.68	1.64	2.39	1.93
Systems Development	1.72	1.97	1.72	2.16	1.64	2.34	1.65	1.65	2.32	1.92
Data Administration	1.82	1.63	1.79	1.62	1.64	1.99	1.73	1.61	2.13	1.81
Knowledge Management	1.84	1.80	1.85	1.68	1.55	2.02	1.72	1.58	2.24	1.79
Customer Service and Technical Support	1.93	1.92	1.93	1.89	1.64	2.18	1.79	1.83	2.83	1.98
Network Services	1.69	1.65	1.55	1.72	1.40	1.82	1.76	1.73	2.15	1.72
System Administration	1.71	1.71	1.66	1.73	1.46	2.07	1.70	1.68	2.44	1.79
Systems Security Analysis	1.70	1.73	1.57	1.66	1.47	1.98	1.70	1.59	2.29	1.69
Computer Network Defense (CND) Analysis	1.56	1.51	1.54	1.56	1.37	1.82	1.59	1.56	2.03	1.62
Incident Response	1.66	1.71	1.58	1.55	1.41	1.91	1.73	1.72	2.21	1.73
Computer Network Defense (CND) Infrastructure Support	1.60	1.49	1.54	1.55	1.37	1.81	1.63	1.61	2.01	1.59
Vulnerability Assessment and Management	1.64	1.71	1.56	1.64	1.39	1.96	1.67	1.66	2.22	1.67
Investigation	1.59	1.66	1.60	1.49	1.45	1.73	2.08	2.42	1.89	1.59
Digital Forensics	1.56	1.49	1.56	1.50	1.43	1.70	1.78	1.89	1.79	1.54
Collection Operations	1.56	1.59	1.62	1.55	1.46	1.72	1.71	1.73	1.86	1.59
Cyber Operations Planning	1.60	1.67	1.57	1.56	1.41	1.72	1.70	1.67	1.87	1.59
Cyber Operations	1.51	1.59	1.59	1.58	1.53	1.65	1.73	1.80	1.80	1.60

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Threat Analysis	1.54	1.66	1.57	1.59	1.40	1.67	1.64	1.69	1.84	1.57
Exploitation Analysis	1.56	1.70	1.55	1.61	1.40	1.79	1.64	1.69	1.91	1.61
All Source Intelligence	1.64	1.70	1.62	1.60	1.64	1.72	1.68	1.80	1.83	1.59
Targets	1.61	1.62	1.65	1.62	1.52	1.64	1.66	1.77	1.82	1.60
Legal Advice and Advocacy	1.61	1.74	1.68	1.54	1.61	1.74	1.77	1.75	1.88	1.61
Strategic Planning and Policy Development	1.76	2.04	1.89	1.71	1.65	1.91	1.73	1.81	2.14	1.75
Education and Training	1.86	1.94	1.90	1.73	1.63	1.89	1.91	1.79	2.21	1.84
Information Systems Security Operations (Information Systems Security Officer [ISSO])	1.67	1.82	1.62	1.66	1.43	1.96	1.68	1.53	2.27	1.70
Security Program Management (Chief Information Security Officer [CISO])	1.61	1.79	1.66	1.63	1.45	1.89	1.67	1.54	2.10	1.65

Table 32: Participants with Advanced/Expert Proficiency - Occupational Series

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Information Assurance (IA) Compliance	6.74%	11.29%	6.61%	14.44%	3.87%	28.84%	6.06%	5.21%	40.42%	10.66%
Software Assurance and Security Engineering	3.15%	5.18%	2.74%	11.11%	1.68%	31.91%	2.60%	1.92%	20.62%	6.63%
Systems Security Architecture	3.97%	8.00%	4.10%	13.06%	1.94%	25.94%	3.16%	3.11%	29.10%	6.84%
Technology Research and Development	4.92%	7.76%	5.30%	25.19%	2.19%	33.45%	3.42%	3.47%	32.64%	9.22%
Systems Requirements Planning	9.59%	14.59%	10.77%	30.09%	3.62%	41.47%	4.95%	3.47%	50.02%	11.89%
Test and Evaluation	6.35%	9.88%	7.86%	30.46%	3.45%	38.74%	4.28%	3.29%	40.39%	10.81%
Systems Development	5.70%	10.35%	6.78%	28.43%	2.44%	39.08%	3.57%	2.74%	35.36%	8.93%
Data Administration	11.75%	7.29%	12.25%	8.98%	5.89%	24.57%	7.25%	5.30%	28.44%	11.24%
Knowledge Management	11.71%	11.29%	12.93%	10.74%	4.21%	23.55%	6.69%	5.02%	34.19%	11.31%
Customer Service and Technical Support	11.27%	12.00%	11.74%	15.56%	5.98%	33.11%	6.02%	5.30%	58.85%	14.12%
Network Services	3.67%	4.94%	3.08%	10.65%	1.35%	15.87%	3.57%	4.02%	27.50%	6.20%
System Administration	3.93%	5.88%	4.10%	10.65%	1.60%	25.09%	3.27%	3.47%	38.59%	7.28%
Systems Security Analysis	3.76%	6.12%	3.19%	8.89%	1.52%	21.84%	3.38%	2.65%	33.74%	5.76%
Computer Network Defense (CND) Analysis	3.41%	4.71%	2.96%	6.11%	1.43%	14.51%	3.83%	3.65%	21.98%	5.91%
Incident Response	5.40%	8.71%	4.44%	6.48%	2.86%	16.38%	6.06%	6.03%	30.28%	8.00%
Computer Network Defense (CND) Infrastructure Support	2.25%	3.06%	2.05%	5.65%	0.59%	13.31%	2.31%	2.37%	20.55%	3.75%
Vulnerability Assessment and Management	3.54%	7.06%	3.48%	7.87%	1.52%	21.16%	3.83%	4.29%	29.91%	5.40%
Investigation	2.72%	4.24%	3.13%	3.70%	1.18%	8.53%	12.27%	38.63%	14.56%	3.60%
Digital Forensics	2.33%	2.82%	2.11%	3.33%	1.26%	8.70%	6.17%	17.90%	11.69%	2.59%
Collection Operations	2.59%	4.47%	3.25%	3.70%	1.26%	8.53%	5.02%	9.95%	13.55%	3.75%
Cyber Operations Planning	1.99%	3.76%	2.68%	3.70%	0.67%	7.51%	3.09%	6.58%	12.62%	2.81%

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Cyber Operations	1.56%	3.29%	2.17%	3.80%	0.93%	6.14%	4.54%	9.86%	10.42%	2.67%
Threat Analysis	1.90%	3.29%	2.39%	3.89%	0.84%	7.34%	4.02%	8.04%	11.71%	2.23%
Exploitation Analysis	2.12%	5.18%	2.74%	4.44%	1.01%	9.22%	4.35%	7.95%	14.66%	2.95%
All Source Intelligence	2.25%	4.71%	2.74%	4.35%	1.35%	7.34%	4.95%	10.14%	11.08%	2.52%
Targets	2.55%	4.00%	3.19%	4.07%	1.35%	6.31%	5.09%	9.95%	10.15%	2.81%
Legal Advice and Advocacy	3.02%	6.82%	4.50%	3.15%	1.94%	6.83%	4.91%	6.03%	12.11%	3.10%
Strategic Planning and Policy Development	7.17%	16.24%	11.45%	6.76%	3.20%	13.99%	5.13%	7.03%	24.00%	5.98%
Education and Training	8.16%	12.94%	10.26%	6.76%	3.96%	13.82%	8.29%	8.04%	27.40%	8.29%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	3.63%	8.47%	3.42%	5.09%	1.26%	14.16%	2.60%	2.92%	26.80%	4.25%
Security Program Management (Chief Information Security Officer [CISO])	3.33%	7.29%	3.65%	3.89%	1.18%	12.12%	2.71%	2.65%	19.92%	3.67%

Table 33: Participants that Meet/Exceed Optimal Proficiency - Occupational Series

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Information Assurance (IA) Compliance	61.31%	59.41%	61.71%	59.16%	68.63%	58.14%	58.90%	56.53%	58.10%	61.76%
Software Assurance and Security Engineering	67.47%	76.92%	62.93%	63.22%	70.30%	60.62%	66.16%	53.33%	57.84%	64.06%
Systems Security Architecture	65.13%	67.80%	65.48%	56.90%	74.17%	55.96%	66.76%	61.01%	56.28%	64.63%
Technology Research and Development	65.49%	68.25%	68.38%	63.79%	65.89%	61.45%	67.30%	62.64%	62.03%	64.96%
Systems Requirements Planning	66.61%	71.60%	67.61%	65.87%	67.33%	60.50%	66.14%	64.07%	66.28%	69.10%
Test and Evaluation	67.86%	69.57%	67.22%	64.07%	71.07%	55.91%	67.88%	59.74%	63.39%	69.34%
Systems Development	70.05%	68.85%	70.07%	66.06%	71.77%	64.17%	67.93%	69.01%	64.79%	70.55%
Data Administration	66.51%	72.29%	67.09%	68.22%	67.27%	60.72%	63.13%	61.43%	64.31%	66.27%
Knowledge Management	68.79%	70.77%	64.84%	66.54%	70.69%	65.68%	62.77%	61.03%	64.19%	68.06%
Customer Service and Technical Support	71.88%	72.97%	72.76%	70.75%	73.59%	73.18%	64.39%	69.05%	76.56%	69.54%
Network Services	68.46%	69.88%	63.95%	65.65%	68.75%	54.13%	69.07%	65.44%	60.41%	61.45%
System Administration	69.71%	68.97%	67.73%	65.00%	68.15%	55.91%	65.80%	60.87%	65.42%	68.71%
Systems Security Analysis	69.77%	63.83%	69.37%	65.12%	70.99%	57.10%	67.71%	63.64%	62.31%	66.67%
Computer Network Defense (CND) Analysis	71.65%	71.72%	74.63%	66.20%	72.14%	57.82%	65.12%	60.19%	57.49%	65.38%
Incident Response	70.32%	75.76%	71.35%	64.09%	72.54%	60.07%	62.78%	56.10%	61.18%	67.82%
Computer Network Defense (CND) Infrastructure Support	70.56%	67.65%	72.04%	63.06%	73.58%	58.24%	63.36%	61.07%	58.02%	62.45%
Vulnerability Assessment and Management	68.31%	70.48%	68.81%	62.50%	76.77%	54.43%	62.81%	57.87%	61.00%	65.10%
Investigation	70.00%	72.15%	71.01%	62.34%	74.12%	58.20%	60.28%	55.70%	55.57%	66.07%
Digital Forensics	66.22%	71.64%	71.05%	66.35%	67.53%	59.49%	60.39%	44.97%	53.60%	65.88%
Collection Operations	65.67%	77.78%	73.33%	65.90%	70.09%	65.08%	62.50%	54.62%	59.65%	69.40%
Cyber Operations Planning	68.32%	66.67%	70.85%	68.29%	63.77%	55.81%	61.39%	50.33%	56.74%	69.14%

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Cyber Operations	65.79%	70.77%	71.52%	67.89%	61.40%	58.08%	60.49%	49.73%	55.89%	66.46%
Threat Analysis	67.00%	79.17%	68.13%	64.82%	75.00%	52.91%	61.93%	49.43%	54.31%	65.93%
Exploitation Analysis	69.67%	77.22%	66.67%	62.73%	75.34%	51.06%	60.38%	47.25%	56.06%	65.57%
All Source Intelligence	71.43%	80.25%	68.14%	59.81%	77.19%	53.66%	58.48%	47.35%	55.03%	63.93%
Targets	69.23%	77.92%	65.48%	65.53%	74.70%	53.21%	61.00%	48.21%	58.02%	67.14%
Legal Advice and Advocacy	69.77%	71.96%	73.13%	66.13%	68.18%	56.25%	61.94%	52.55%	57.72%	68.18%
Strategic Planning and Policy Development	70.70%	69.68%	68.25%	63.14%	71.09%	61.09%	60.99%	55.93%	60.63%	68.61%
Education and Training	74.25%	71.52%	71.70%	67.03%	70.88%	64.22%	61.82%	54.88%	65.44%	74.77%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	67.44%	74.11%	71.54%	64.90%	69.90%	58.72%	65.81%	57.53%	63.32%	65.45%
Security Program Management (Chief Information Security Officer [CISO])	67.33%	70.37%	70.39%	68.57%	68.27%	58.59%	64.04%	57.75%	59.29%	71.16%

Table 34: Average Proficiency by 2210 Series Primary Parenthetical Titles

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Information Assurance (IA) Compliance	2.04	2.02	2.23	2.30	2.10	2.30	2.42	2.36	3.07	2.38	2.12
Software Assurance and Security Engineering	2.50	1.69	2.23	1.95	2.30	1.71	2.05	1.81	1.98	1.89	1.96
Systems Security Architecture	2.15	1.83	2.16	2.37	2.21	2.20	2.28	2.11	2.49	2.12	2.02
Technology Research and Development	2.23	2.01	2.31	2.54	2.16	2.31	2.44	2.22	2.43	2.21	2.16
Systems Requirements Planning	2.70	2.34	2.58	2.86	2.38	2.62	2.77	2.69	2.67	2.51	2.66
Test and Evaluation	2.62	2.13	2.40	2.42	2.22	2.34	2.57	2.30	2.57	2.35	2.41
Systems Development	2.68	1.97	2.49	2.58	2.13	2.14	2.35	2.24	2.36	2.22	2.41
Data Administration	2.32	1.98	2.91	2.09	2.09	2.03	2.19	1.98	2.02	2.20	2.09
Knowledge Management	2.22	2.12	2.55	2.34	2.37	2.20	2.36	2.28	2.27	2.32	2.20
Customer Service and Technical Support	2.67	3.11	2.88	2.64	2.69	3.03	3.03	2.66	2.75	3.16	2.66
Network Services	1.80	2.13	1.80	2.31	1.94	2.79	2.25	2.02	2.27	2.31	1.97

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
System Administration	2.06	2.41	2.31	2.53	2.40	2.60	2.68	2.18	2.49	3.03	2.22
Systems Security Analysis	2.00	2.06	2.17	2.34	2.00	2.40	2.26	2.09	2.74	2.51	2.11
Computer Network Defense (CND) Analysis	1.69	1.85	1.75	1.93	1.82	2.11	1.96	1.99	2.51	2.04	1.80
Incident Response	1.79	2.12	1.91	2.15	1.81	2.28	2.26	2.12	2.70	2.29	1.96
Computer Network Defense (CND) Infrastructure Support	1.69	1.84	1.73	2.00	1.76	2.23	1.99	1.99	2.38	2.05	1.83
Vulnerability Assessment and Management	1.77	1.93	1.95	2.12	1.96	2.26	2.10	2.11	2.87	2.21	1.98
Investigation	1.73	1.81	1.59	1.86	1.66	1.89	1.83	1.88	2.16	1.89	1.74
Digital Forensics	1.67	1.71	1.59	1.73	1.71	1.78	1.62	1.76	2.01	1.78	1.68
Collection Operations	1.75	1.74	1.78	1.88	1.65	1.81	1.96	1.87	2.11	1.84	1.69
Cyber Operations Planning	1.65	1.73	1.72	1.91	1.67	1.81	1.80	1.94	2.17	1.74	1.66
Cyber Operations	1.70	1.71	1.66	1.85	1.56	1.78	1.58	1.81	2.02	1.74	1.67
Threat Analysis	1.71	1.71	1.60	1.72	1.87	1.76	1.79	1.76	2.15	1.76	1.69

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Exploitation Analysis	1.69	1.70	1.67	1.81	1.91	1.81	1.94	1.87	2.32	1.78	1.77
All Source Intelligence	1.67	1.74	1.66	1.67	1.79	1.68	1.87	1.82	2.09	1.72	1.69
Targets	1.65	1.80	1.63	1.64	1.87	1.76	1.84	1.85	2.04	1.74	1.68
Legal Advice and Advocacy	1.70	1.74	1.64	1.73	1.56	1.75	1.72	2.01	2.14	1.81	1.68
Strategic Planning and Policy Development	1.81	1.87	1.82	2.18	1.85	2.11	2.08	2.47	2.42	1.97	1.96
Education and Training	1.91	2.01	2.03	2.15	2.16	2.20	2.19	2.41	2.54	2.06	2.08
Information Systems Security Operations (Information Systems Security Officer [ISSO])	1.81	2.00	1.87	2.21	1.97	2.12	1.91	2.26	2.92	2.09	1.94
Security Program Management (Chief Information Security Officer [CISO])	1.68	1.86	1.71	1.94	1.91	1.98	1.87	2.14	2.59	1.92	1.77

Table 35: Participants with Advanced/Expert Proficiency - 2210 Series Parenthetical Titles

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Information Assurance (IA) Compliance	26.85%	26.32%	35.65%	37.50%	25.93%	41.18%	39.05%	40.67%	72.36%	43.50%	29.74%
Software Assurance and Security Engineering	44.66%	9.55%	32.81%	20.39%	32.10%	13.30%	23.81%	13.02%	20.36%	18.79%	20.42%
Systems Security Architecture	30.00%	15.30%	29.65%	41.45%	20.99%	32.99%	30.48%	25.76%	45.03%	29.21%	26.31%
Technology Research and Development	35.75%	20.81%	35.02%	48.03%	27.16%	36.83%	40.00%	29.96%	41.35%	32.30%	29.90%
Systems Requirements Planning	56.85%	37.33%	52.05%	61.18%	38.27%	52.43%	51.43%	53.69%	54.19%	48.13%	54.74%
Test and Evaluation	51.92%	26.07%	41.96%	42.11%	34.57%	40.66%	41.90%	35.46%	49.10%	39.38%	42.81%
Systems Development	53.97%	19.83%	44.48%	46.71%	32.10%	30.69%	33.33%	30.39%	38.29%	32.82%	39.05%
Data Administration	36.30%	21.42%	64.98%	27.63%	29.63%	25.32%	24.76%	22.29%	23.81%	35.26%	25.98%
Knowledge Management	33.42%	27.91%	51.10%	35.53%	38.27%	35.81%	39.05%	35.46%	35.94%	39.77%	32.68%
Customer Service and Technical Support	52.05%	72.95%	65.62%	48.68%	48.15%	70.08%	66.67%	48.05%	56.15%	77.99%	50.16%
Network Services	12.19%	28.64%	16.09%	32.24%	18.52%	59.85%	29.52%	23.01%	33.67%	38.48%	18.63%
System Administration	22.19%	38.92%	33.75%	42.11%	30.86%	51.92%	45.71%	27.93%	43.23%	70.91%	28.10%
Systems Security	20.41%	24.11%	30.28%	34.21%	18.52%	41.43%	36.19%	25.04%	56.30%	46.72%	25.98%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Analysis											
Computer Network Defense (CND) Analysis	9.04%	16.65%	14.51%	17.76%	16.05%	30.95%	15.24%	20.12%	45.42%	24.97%	12.25%
Incident Response	13.29%	27.29%	21.14%	32.24%	16.05%	37.08%	32.38%	26.05%	55.13%	37.07%	18.63%
Computer Network Defense (CND) Infrastructure Support	8.63%	14.57%	11.99%	25.00%	14.81%	33.76%	19.05%	18.38%	38.14%	24.71%	13.40%
Vulnerability Assessment and Management	12.33%	18.60%	20.50%	30.26%	20.99%	36.57%	26.67%	25.90%	63.74%	32.69%	18.30%
Investigation	8.08%	11.87%	7.89%	14.47%	8.64%	17.90%	11.43%	14.04%	27.56%	15.83%	9.31%
Digital Forensics	7.12%	9.30%	7.57%	9.87%	8.64%	14.83%	7.62%	9.70%	22.24%	13.26%	7.68%
Collection Operations	8.08%	9.55%	11.36%	13.82%	6.17%	15.60%	11.43%	14.33%	25.76%	14.03%	8.33%
Cyber Operations Planning	6.16%	7.96%	8.52%	17.11%	6.17%	13.04%	7.62%	15.63%	26.94%	9.78%	6.70%
Cyber Operations	5.62%	7.22%	7.57%	13.16%	3.70%	12.79%	5.71%	11.29%	20.99%	9.14%	6.37%
Threat Analysis	6.16%	7.71%	7.26%	9.87%	8.64%	12.02%	7.62%	9.99%	26.39%	10.42%	7.03%
Exploitation Analysis	7.26%	8.81%	10.09%	10.53%	8.64%	13.55%	13.33%	12.74%	35.08%	12.87%	8.99%
All Source Intelligence	5.89%	8.57%	6.62%	7.24%	7.41%	9.97%	9.52%	11.58%	24.20%	9.01%	6.70%
Targets	5.48%	8.45%	6.62%	8.55%	7.41%	10.49%	9.52%	11.00%	20.05%	8.37%	6.37%
Legal Advice and Advocacy	5.62%	8.57%	6.62%	11.84%	4.94%	11.25%	10.48%	17.80%	24.43%	10.55%	6.05%
Strategic	11.92%	13.59%	14.83%	32.24%	14.81%	22.25%	21.90%	42.98%	40.41%	17.89%	17.32%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Planning and Policy Development											
Education and Training	14.52%	19.58%	19.87%	27.63%	18.52%	28.13%	24.76%	38.21%	47.45%	24.20%	20.75%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	9.18%	16.89%	14.83%	25.66%	11.11%	26.60%	13.33%	29.81%	62.80%	23.94%	15.52%
Security Program Management (Chief Information Security Officer [CISO])	6.16%	11.63%	8.52%	21.71%	8.64%	19.69%	13.33%	26.77%	46.28%	16.22%	9.15%

Table 36: Participants that Meet/Exceed Optimal Proficiency - 2210 Series Parenthetical Titles

Specialty Areas	2210 Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Information Assurance (IA) Compliance	54.81%	58.35%	61.57%	61.54%	45.83%	56.82%	58.11%	59.19%	61.55%	57.29%	54.73%
Software Assurance and Security Engineering	57.65%	60.20%	59.90%	56.82%	50.00%	60.50%	62.71%	63.21%	52.48%	54.11%	58.82%
Systems Security Architecture	52.73%	56.16%	60.29%	59.65%	60.98%	59.85%	54.41%	59.72%	54.17%	55.69%	56.23%
Technology Research and Development	59.63%	65.56%	65.24%	63.64%	58.70%	63.24%	60.29%	65.32%	58.53%	61.68%	61.72%
Systems Requirements Planning	67.54%	68.10%	66.81%	67.23%	53.85%	66.22%	65.75%	69.23%	63.91%	64.61%	67.60%
Test and Evaluation	62.99%	63.74%	66.06%	68.14%	58.33%	61.17%	57.97%	66.44%	60.48%	62.05%	64.89%
Systems Development	67.24%	64.10%	68.18%	68.14%	59.09%	62.78%	60.61%	69.71%	61.24%	60.86%	62.75%

Specialty Areas	2210 Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Data Administration	64.43%	64.53%	70.20%	67.96%	57.45%	64.06%	60.34%	68.06%	62.41%	59.44%	63.49%
Knowledge Management	62.63%	67.93%	65.11%	68.75%	66.67%	67.13%	62.69%	67.89%	60.42%	62.89%	61.02%
Customer Service and Technical Support	77.30%	76.67%	75.63%	83.96%	68.63%	76.27%	78.67%	76.65%	75.94%	77.23%	75.35%
Network Services	54.63%	62.39%	64.24%	70.79%	50.00%	62.62%	54.24%	60.22%	58.49%	58.67%	60.26%
System Administration	58.43%	65.63%	71.81%	78.26%	52.78%	63.39%	63.08%	67.69%	63.50%	68.35%	61.89%
Systems Security Analysis	60.05%	62.74%	65.78%	70.33%	69.44%	61.89%	58.46%	65.05%	63.44%	59.19%	60.86%
Computer Network Defense (CND) Analysis	57.09%	64.02%	58.71%	57.65%	70.27%	52.43%	53.57%	62.18%	54.50%	54.27%	55.71%
Incident Response	60.62%	66.23%	66.12%	60.23%	57.50%	59.71%	58.46%	58.22%	61.41%	58.24%	59.34%

Specialty Areas	2210 Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Computer Network Defense (CND) Infrastructure Support	58.27%	61.21%	61.48%	59.49%	72.22%	55.34%	50.98%	59.32%	56.26%	57.20%	54.58%
Vulnerability Assessment and Management	57.43%	63.82%	63.19%	58.70%	64.86%	59.12%	58.46%	60.37%	63.55%	59.77%	58.14%
Investigation	56.72%	58.91%	61.11%	61.19%	61.54%	53.85%	54.76%	61.07%	50.53%	55.85%	55.39%
Digital Forensics	58.03%	60.38%	56.73%	57.14%	59.09%	49.50%	51.22%	57.49%	46.62%	55.01%	55.26%
Collection Operations	60.66%	61.83%	63.72%	69.44%	60.87%	58.06%	65.85%	61.45%	56.93%	56.91%	53.85%
Cyber Operations Planning	57.14%	59.72%	61.00%	63.89%	58.33%	55.00%	52.50%	61.01%	53.41%	54.87%	55.43%
Cyber Operations	57.83%	59.09%	57.29%	59.32%	50.00%	55.49%	48.72%	61.84%	49.78%	54.67%	58.64%
Threat Analysis	56.71%	55.45%	54.84%	58.06%	54.55%	57.65%	47.22%	56.97%	51.14%	50.72%	54.65%
Exploitation Analysis	55.77%	58.87%	59.22%	57.14%	60.00%	56.08%	57.89%	60.89%	52.46%	50.92%	56.48%
All Source Intelligence	56.73%	53.09%	56.10%	56.90%	55.00%	57.23%	57.14%	55.56%	52.10%	54.31%	53.09%
Targets	59.39%	58.03%	62.92%	55.93%	68.18%	59.38%	66.67%	62.22%	53.88%	57.25%	53.37%

Specialty Areas	2210 Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Legal Advice and Advocacy	57.06%	62.69%	58.33%	52.94%	73.91%	53.57%	54.29%	61.54%	55.45%	57.42%	54.76%
Strategic Planning and Policy Development	62.17%	64.60%	61.43%	55.88%	60.61%	59.13%	67.35%	63.62%	57.08%	56.02%	59.43%
Education and Training	63.04%	66.03%	65.79%	63.04%	76.67%	61.64%	70.21%	67.54%	65.15%	61.31%	63.81%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	58.33%	69.05%	58.54%	62.50%	70.37%	61.64%	56.82%	61.33%	68.13%	57.61%	57.36%
Security Program Management (Chief Information Security Officer [CISO])	56.42%	61.00%	54.72%	55.13%	68.18%	60.50%	58.54%	60.28%	59.84%	54.60%	57.49%

Table 37: Training Needs by Pay Grade

Specialty Area	Pay Grade						
	GS 4 and below	GS 5-10	GS 11-13	GS 14-15	SES	SL/ST	Other
Information Assurance (IA) Compliance	29.27%	21.74%	28.64%	25.87%	15.63%	17.95%	22.30%
Software Assurance and Security Engineering	4.88%	7.34%	11.92%	10.87%	3.13%	12.82%	9.21%
Systems Security Architecture	12.20%	8.63%	15.17%	17.80%	11.46%	23.08%	10.01%
Technology Research and Development	9.76%	6.83%	10.22%	10.05%	6.77%	20.51%	9.35%
Systems Requirements Planning	4.88%	6.79%	15.31%	16.42%	6.77%	10.26%	9.48%
Test and Evaluation	21.95%	9.86%	15.46%	12.07%	4.69%	10.26%	13.75%
Systems Development	7.32%	8.09%	13.67%	12.56%	5.73%	10.26%	9.35%
Data Administration	12.20%	19.45%	17.88%	12.43%	5.73%	2.56%	13.62%
Knowledge Management	17.07%	16.38%	18.09%	19.92%	21.35%	23.08%	15.62%
Customer Service and Technical Support	26.83%	19.18%	13.63%	7.25%	5.21%	2.56%	10.81%
Network Services	14.63%	11.71%	15.02%	7.97%	4.17%	7.69%	13.48%
System Administration	9.76%	14.44%	17.05%	8.43%	4.17%	2.56%	13.08%
Systems Security Analysis	4.88%	7.71%	12.81%	11.07%	5.73%	7.69%	9.75%
Computer Network Defense (CND) Analysis	7.32%	6.21%	9.82%	8.79%	5.73%	7.69%	6.41%
Incident Response	24.39%	13.86%	16.31%	14.80%	20.83%	7.69%	17.62%
Computer Network Defense (CND) Infrastructure Support	17.07%	6.21%	9.27%	7.23%	6.77%	10.26%	6.14%
Vulnerability Assessment and Management	7.32%	13.55%	20.74%	20.80%	18.23%	10.26%	21.23%
Investigation	4.88%	13.65%	16.63%	13.68%	15.63%	12.82%	14.29%

Specialty Area	Pay Grade						
	GS 4 and below	GS 5-10	GS 11-13	GS 14-15	SES	SL/ST	Other
Digital Forensics	2.44%	9.97%	14.38%	11.91%	11.46%	10.26%	9.88%
Collection Operations	4.88%	6.86%	8.17%	6.29%	6.77%	2.56%	5.61%
Cyber Operations Planning	7.32%	4.44%	7.66%	9.79%	9.90%	12.82%	5.07%
Cyber Operations	9.76%	6.38%	10.29%	10.19%	10.42%	10.26%	6.68%
Threat Analysis	2.44%	12.42%	16.19%	15.74%	17.71%	23.08%	15.49%
Exploitation Analysis	2.44%	5.05%	8.73%	8.51%	7.29%	2.56%	6.94%
All Source Intelligence	12.20%	6.69%	8.36%	8.61%	12.50%	10.26%	7.61%
Targets	24.39%	4.95%	6.31%	5.53%	9.38%	2.56%	5.61%
Legal Advice and Advocacy	7.32%	5.22%	6.82%	8.67%	11.46%	10.26%	4.41%
Strategic Planning and Policy Development	6.56%	5.56%	10.03%	19.76%	23.96%	25.64%	7.08%
Education and Training	16.50%	20.38%	16.96%	13.44%	13.54%	12.82%	19.49%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	4.97%	9.15%	12.81%	11.01%	8.33%	12.82%	8.14%
Security Program Management (Chief Information Security Officer [CISO])	3.31%	4.91%	7.89%	11.67%	10.94%	17.95%	5.34%

Table 38: Training Needs by Occupational Series

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Information Assurance (IA) Compliance	16.54%	16.47%	15.50%	36.94%	9.51%	38.91%	13.54%	11.14%	44.65%	17.00%
Software Assurance and Security Engineering	4.02%	4.71%	4.22%	20.00%	2.44%	34.13%	3.31%	3.11%	18.88%	6.34%
Systems Security Architecture	4.67%	6.35%	4.62%	24.54%	1.77%	27.30%	4.80%	4.38%	28.41%	7.20%
Technology Research and Development	4.58%	6.35%	5.87%	20.46%	2.44%	23.04%	3.98%	3.56%	15.31%	5.76%
Systems Requirements Planning	7.86%	12.24%	12.31%	24.81%	3.37%	24.91%	3.90%	2.83%	23.35%	7.93%
Test and Evaluation	7.34%	9.18%	9.34%	28.24%	5.22%	27.99%	7.10%	3.93%	20.18%	9.73%
Systems Development	6.87%	8.24%	8.32%	25.28%	3.79%	25.26%	5.09%	3.20%	18.89%	8.93%
Data Administration	22.76%	10.35%	20.80%	8.15%	13.89%	14.16%	12.76%	6.21%	19.14%	14.91%
Knowledge Management	22.63%	22.82%	26.15%	10.09%	12.04%	14.85%	14.88%	8.13%	20.44%	17.44%
Customer Service and Technical Support	12.35%	7.76%	9.86%	3.70%	12.37%	6.14%	6.47%	3.20%	20.24%	14.48%
Network Services	5.23%	4.24%	4.50%	13.80%	4.46%	18.60%	5.91%	8.13%	23.58%	9.65%
System Administration	8.68%	8.47%	7.64%	11.30%	5.39%	18.60%	6.88%	5.75%	26.45%	10.09%
Systems Security Analysis	3.46%	5.88%	4.39%	11.85%	1.60%	16.72%	6.84%	7.95%	22.42%	6.63%
Computer Network Defense (CND) Analysis	2.76%	2.35%	1.94%	7.50%	0.76%	15.19%	3.90%	9.04%	18.55%	4.68%
Incident Response	11.40%	14.59%	8.55%	4.91%	8.33%	9.56%	21.16%	26.30%	21.95%	13.40%
Computer Network Defense (CND) Infrastructure Support	2.68%	2.12%	1.54%	6.76%	1.09%	12.29%	3.57%	8.22%	17.22%	4.11%
Vulnerability Assessment and Management	11.75%	21.18%	10.88%	16.11%	9.34%	23.89%	19.71%	18.36%	30.28%	12.82%
Investigation	6.74%	6.59%	6.55%	4.35%	2.61%	7.85%	34.62%	65.84%	13.76%	6.99%
Digital Forensics	3.93%	4.00%	3.82%	6.30%	2.19%	10.92%	16.25%	46.12%	18.02%	5.76%
Collection Operations	3.84%	2.82%	5.01%	3.24%	1.85%	4.95%	11.79%	25.21%	8.33%	3.31%
Cyber Operations Planning	3.50%	3.29%	3.93%	5.09%	0.51%	9.22%	5.09%	15.43%	13.69%	3.03%

Specialty Area	Occupational Series									
	0301	0340	0343	0855	1101	1550	1801	1811	2210	Other
Cyber Operations	4.41%	3.53%	4.16%	6.76%	1.60%	10.58%	8.07%	23.47%	15.76%	3.75%
Threat Analysis	7.69%	10.82%	8.72%	10.83%	6.57%	16.55%	23.09%	31.69%	19.27%	10.45%
Exploitation Analysis	2.68%	4.24%	3.13%	5.74%	0.76%	9.22%	8.63%	19.63%	12.62%	3.31%
All Source Intelligence	3.59%	3.76%	4.50%	3.98%	1.35%	7.00%	18.41%	26.48%	7.15%	3.53%
Targets	2.55%	4.24%	2.62%	3.52%	1.77%	4.78%	12.72%	20.82%	5.12%	2.38%
Legal Advice and Advocacy	6.35%	6.82%	5.53%	2.78%	2.10%	5.46%	9.71%	12.15%	8.89%	4.32%
Strategic Planning and Policy Development	10.63%	20.94%	18.46%	6.76%	4.21%	9.22%	8.07%	7.21%	16.36%	6.56%
Education and Training	18.53%	16.00%	17.72%	6.94%	17.17%	9.04%	22.20%	19.18%	16.04%	16.50%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	5.31%	7.06%	5.75%	6.48%	2.19%	13.14%	5.73%	6.12%	23.95%	4.97%
Security Program Management (Chief Information Security Officer [CISO])	3.50%	7.53%	4.39%	3.89%	1.18%	8.19%	4.02%	5.57%	16.79%	3.31%

Table 39: Training Needs by 2210 Primary Parenthetical Title

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Information Assurance (IA) Compliance	39.73%	41.37%	41.32%	45.39%	39.51%	43.22%	41.90%	47.32%	54.66%	45.56%	41.67%
Software Assurance and Security Engineering	38.08%	11.75%	19.56%	19.74%	25.93%	11.51%	17.14%	12.74%	22.24%	14.16%	18.46%
Systems Security Architecture	29.59%	18.12%	28.08%	50.00%	30.86%	29.67%	32.38%	22.43%	38.14%	30.50%	25.98%
Technology Research and Development	21.92%	12.73%	17.67%	26.97%	24.69%	15.35%	18.10%	15.92%	11.51%	11.20%	17.65%
Systems Requirements Planning	30.96%	18.12%	20.19%	34.21%	27.16%	23.53%	21.90%	30.25%	17.31%	18.92%	33.17%
Test and Evaluation	32.60%	18.36%	17.35%	17.11%	22.22%	16.88%	24.76%	12.30%	20.44%	16.09%	24.84%
Systems Development	35.34%	12.36%	22.71%	22.37%	28.40%	13.30%	20.95%	14.18%	12.69%	18.66%	26.31%
Data Administration	25.89%	18.60%	54.57%	13.16%	32.10%	13.30%	13.33%	10.56%	10.34%	23.42%	19.12%
Knowledge Management	16.99%	23.75%	26.81%	25.66%	33.33%	18.41%	17.14%	31.40%	14.80%	17.63%	20.42%
Customer Service and Technical Support	13.97%	49.94%	18.61%	13.82%	18.52%	20.46%	20.95%	14.62%	8.30%	25.61%	17.32%
Network Services	13.01%	35.13%	14.20%	15.13%	14.81%	51.92%	18.10%	14.18%	20.52%	35.01%	18.14%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
System Administration	18.08%	35.86%	27.44%	12.50%	28.40%	34.53%	25.71%	14.18%	18.72%	53.93%	22.88%
Systems Security Analysis	19.18%	17.99%	21.14%	15.79%	17.28%	20.72%	24.76%	14.76%	34.30%	28.06%	22.22%
Computer Network Defense (CND) Analysis	10.14%	13.71%	13.56%	14.47%	9.88%	25.58%	21.90%	18.38%	33.75%	21.11%	12.09%
Incident Response	10.41%	26.93%	11.99%	11.84%	22.22%	25.06%	20.00%	16.79%	37.04%	24.20%	13.89%
Computer Network Defense (CND) Infrastructure Support	7.53%	13.71%	10.09%	18.42%	11.11%	31.71%	19.05%	17.80%	27.64%	19.31%	11.93%
Vulnerability Assessment and Management	21.37%	27.05%	25.24%	26.97%	20.99%	33.76%	26.67%	26.63%	45.42%	34.88%	25.16%
Investigation	7.26%	13.10%	9.78%	10.53%	14.81%	16.37%	15.24%	9.99%	26.08%	14.54%	9.31%
Digital Forensics	8.77%	15.91%	12.93%	13.82%	17.28%	19.69%	21.90%	12.45%	34.69%	21.49%	10.13%
Collection Operations	5.07%	9.67%	7.26%	7.24%	9.88%	8.18%	17.14%	5.50%	13.23%	9.65%	5.23%
Cyber Operations Planning	7.53%	11.51%	8.20%	19.74%	14.81%	15.60%	18.10%	18.96%	23.26%	10.30%	8.01%
Cyber Operations	9.86%	12.97%	10.09%	15.13%	12.35%	19.18%	20.00%	16.64%	27.88%	15.32%	10.46%
Threat Analysis	15.34%	17.87%	13.88%	19.08%	18.52%	17.39%	19.05%	12.45%	35.40%	18.53%	13.24%

Specialty Area	2210 Primary Parenthetical Titles										
	Applications Software	Customer Support	Data Management	Enterprise Architecture	Internet	Network Services	Operating Systems	Policy and Planning	Security	Systems Administration	Systems Analysis
Exploitation Analysis	9.45%	9.06%	8.20%	12.50%	18.52%	10.49%	15.24%	8.25%	26.23%	12.10%	8.01%
All Source Intelligence	5.07%	6.98%	5.36%	5.92%	6.17%	6.14%	8.57%	6.95%	13.86%	5.28%	3.43%
Targets	3.29%	5.63%	2.21%	5.92%	7.41%	5.37%	7.62%	5.21%	9.01%	4.50%	2.61%
Legal Advice and Advocacy	4.93%	5.63%	2.84%	10.53%	8.64%	7.16%	5.71%	13.31%	15.90%	6.44%	5.88%
Strategic Planning and Policy Development	9.73%	8.69%	7.89%	37.50%	16.05%	12.53%	18.10%	36.18%	21.30%	7.46%	13.56%
Education and Training	12.47%	22.89%	14.20%	13.16%	20.99%	16.11%	15.24%	16.64%	16.68%	16.86%	13.40%
Information Systems Security Operations (Information Systems Security Officer [ISSO])	17.67%	22.15%	19.87%	19.74%	18.52%	27.11%	21.90%	22.00%	37.35%	28.31%	17.97%
Security Program Management (Chief Information Security Officer [CISO])	8.90%	10.40%	9.78%	17.76%	11.11%	14.32%	13.33%	20.84%	35.71%	13.13%	8.82%

Appendix D: ITWAC Questions

OCCUPATIONAL PROFILE

What is your home agency or department?

Within your home agency, what is the name of the highest level organizational component where you work?

Please specify your highest level organizational component:

Within your highest level organizational component, what is the name of the office where you work?

Please specify your office name:

Within your office, what is the name of the sub-office where you work?

Please specify your sub-office name:

What is your official occupational series? (Use the Office of Personnel Management (OPM) occupational list provided below. If your agency does not use OPM Occupational Series, please select "Other" and type in your occupational information.)

Please specify your occupational series:

What is the basic title associated with your 2210 series position?

What is your primary 2210 series parenthetical title?
To provide additional detail about the work, parenthetical titles are used with the basic title to further identify the duties and responsibilities performed and the special knowledge and skills needed. Any combination of two parenthetical specialty titles may be used in official position titles; Please choose the one or two parenthetical title(s) that apply to you. If you do not have a designated parenthetical title, please select "None" from the response options and continue.

What is your secondary 2210 series parenthetical title?

What is your current General Schedule/Senior Executive Service or equivalent pay grade?

Please specify your pay plan and grade:

What is your employee type?
Active Duty Military: Individuals on active duty, including members of the National Guard and Reserve Components who have been called to active duty, with one of the

U.S. military services: Air Force, Army, Coast Guard, Marine Corps, or Navy. (For these purposes "Military" is equivalent to "Armed Forces" as defined at 5 U.S.C. § 2101).

Federal Civilian Service - Non-Foreign Service: Federal Civil Service - Non-Foreign Service: The Federal civil service includes all appointive positions in the executive, judicial, and legislative branches of the Federal Government, except positions in the uniformed services. (5 U.S.C. § 2101).

Federal Civilian Service - Foreign Service: Federal Civil Service - Foreign Service: The Foreign Service is the subset of Federal civil service established in the Foreign Service Act of 1980 (P.L. 96-465). Foreign Service employees are United States citizens who serve abroad as Chiefs of Mission, Ambassadors at Large, members of the Senior Foreign Service, Foreign Service Officers, Foreign Service Specialists or personnel, and consular agents. The Foreign Service also includes foreign nationals who provide clerical, administrative, technical, fiscal, and other support at Foreign Service posts abroad.

What is your Supervisor Status (according to OPM classification)?
Supervisor or Manager: Position requires the exercise of supervisory or managerial responsibilities that meet, at least, the minimum requirements for application of the General Schedule Supervisory Guide or similar standards of minimum supervisory responsibility specified by position classification standards or other directives of the applicable pay schedule or system.

Team Leader: Position is titled with the prefix "Lead" and meets the minimum requirements for application of the General Schedule Team Leader Grade-Evaluation Guide; position leads a team of General Schedule employees performing two-grade interval work.

All Other Positions: Position does not meet the above definition of Supervisor or Manager, Leader, or Team Leader.

How soon are you eligible for retirement?

CYBERSECURITY COMPETENCIES
Specialty Areas describe groupings of highly related knowledge skills and abilities that make up the field of cybersecurity. In this section, you will be asked to make two entries for each Specialty Area.

For each Specialty Area described below:

First, indicate your current Proficiency Level using the provided scale. These are the cybersecurity competencies you currently possess. Your rating should **not** be influenced by your current work responsibilities or how you have achieved your proficiency (e.g., activities, personal development, employment, training, education, etc.).

Second, think about your current work responsibilities. For each Specialty Area, please indicate the optimal Proficiency Level for someone in your role at your organization. This level may be the same, lower, or higher than the level you indicated for your current Proficiency Level.

What Specialty Areas describe your current work responsibilities?
Please check the box next to each Specialty Area that falls within your current work responsibilities. You do not need to perform everything described in a Specialty Area. However, the descriptions should account for a large part of your work.

Percentage of Cybersecurity and Other Work
The Cybersecurity Specialty Area(s) that you have said best describe your work are listed below. You may also perform work in other areas not related to Cybersecurity, therefore, an "All Other Work Not Related to Cybersecurity" category is provided so that you can account for 100% of your time.

Please assign a percentage that generally represents the amount of time you spend performing work (over the course of a year) in the Cybersecurity Specialty Area(s) and the other activities.

Your answers must total 100%

Criticality of Specialty Areas
The Cybersecurity Specialty Area(s) that you have said best describe your work are listed below. You may also perform work in other areas not related to Cybersecurity, therefore, an "All Other Work Not Related to Cybersecurity" category is provided. With 1 being the most important, please rank the Cybersecurity Specialty Area(s) and other work in terms of how critical they are to executing the responsibilities of your current job. Each rank may only be used once.

WORK EXPERIENCE

How many years have you performed cybersecurity-related work in the following settings (please indicate the total number of years in each setting)?
The Federal Government includes active military, political appointees, and any full-time/part-time/seasonal Federal employees including those hired through special hiring authorities. It does not include Federal contractors or consultants, detailed SLTT employees, or 1099s.

SLTT government includes any full-time/part-time/seasonal employees, administrators, or appointees that work in SLTT governmental institutions (which excludes academic organizations).

Private Sector/Self-Employed settings include corporate, small business, non-profit, consulting/contracting employees and self-employed individuals.

Academia includes university and college settings (public or private), and academia affiliated research centers.

How many years have you worked for the Federal Government in any capacity (military and civilian years should be combined)?

CERTIFICATIONS
Please enter all of your cybersecurity-related certifications. Click "Add Certification" to begin and again to add additional certifications. The certifications you add will appear in a list below. When all of your certifications have been added, click "Save and Continue." If you have no certifications, please click "Continue."

ADD CERTIFICATION
Please begin by providing details on a certification that you hold. You will have the opportunity to add any additional certifications on the next page. When you have finished entering the information related to this certification, please scroll down to bottom and click "Save."

- A standardized qualification – garnered through testing – that one possesses the necessary KSAs and experience to take on a specific kind of task, typically evaluated by a third party.

Certification:

Other Certification:

Latest Year Certified:

EDUCATION
Have you received any academic degrees since high school?
Official recognition conferred by a college, university, or other postsecondary education institution for the successful completion of a program of studies.

ACADEMIC DEGREE
Please provide information below regarding the education you have completed since high school.
Please select all your completed Academic Degrees. (choose the subject that most closely matches your degree)

Non-Degree Cybersecurity Program
Non-degree program types include: Cybersecurity-related Military Training Program, and Certificate Program.

A course or a combination of courses and related activities offered by a military institution for the attainment of cybersecurity competencies intended for job-related use (not general awareness or safe practices training).

A formal verification – garnered through a course of study – that one received training/education in specific KSAs. This course of study does not include testing resulting in qualification of degree of certification.

Have you completed a cybersecurity-related military training program (not general awareness or safe practices training)?

Have you completed a cybersecurity-related Certificate Program?

TRAINING
In which Specialty Areas would additional training make you more effective in your current job? (Check all that apply) (Click on the "?" to see the definition of each specialty area)

Enter any other training you may need to meet your current job responsibilities related to cybersecurity not listed above.

With 1 being the most important, please rank, in order of priority, your selected training that would make you more effective in your current job.

DEMOGRAPHICS
Please fill out the demographics questions below. Although optional, responses to these questions will enhance our understanding of the cybersecurity workforce.

Please select your gender.

Please select your current age from the ranges.

With which ethnicity do you most closely identify?

With which race/national origin do you identify?

Do you have targeted disability status?
The EEOC defines targeted disabilities as deafness, blindness, missing extremities, partial paralysis, complete paralysis, convulsive disorders, intellectual disability, mental illness and genetic or physical conditions affecting the limbs and/or spine.

Are you a veteran?

This concludes the assessment. Clicking "Submit" below submits your responses.

THANK YOU AND SUMMARY

Did you participate in the 2011 IT Workforce Capability Assessment (ITWCA) sponsored by the Federal Chief Information Officers Council?

- Yes
- No
- Don't Know

Please rate the extent to which you agree with the following statements about this assessment.

It was easy for me to understand the NICE framework.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

It was easy for me to navigate the assessment.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

Please provide any additional comments, feedback, suggestions you have in the text box below:

Appendix E: Specialty Area Behavioral Indicators

Below are the Specialty Area definitions and Behavioral Indicators for reference to assist users in determining their proficiency level in all Specialty Areas that make up the Framework.

Table 40: ITWAC Behavioral Indicators

Systems Security Architecture	Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
BEHAVIORAL INDICATORS	
1 Basic	• Researches current or emerging technologies for security, compatibility, and/or usability purposes • Participates in the security review process by applying basic knowledge of systems testing and evaluation methods for security review; documents gaps found in security architecture to inform the risk management plan • Uses basic data gathering skills to document design specifications and user needs; reports findings that contribute to the systems development lifecycle and enterprise architecture activities and decisions
2 Intermediate	• Assesses user needs and requirements, and interprets and uses IT architectural guidelines to review system architecture designs or system • Documents design specifications, installation instructions, and other system-related information to integrate and migrate existing and planned platforms in support of an organization's enterprise architecture • Discerns protection needs (e.g., security controls) to compare an organization's protection requirements to its information security guidance; identifies gaps in its security architecture, presents considerations for applicability and risk, and provides recommendations for remediation
3 Advanced	• Analyzes similarities and differences of an existing system and customer needs to identify protection needs for information system(s) and network(s); provides detailed specifications for technical needs of the infrastructure • Develops a system security context and preliminary system security concept of operations (CONOPS), including baseline system security requirements • Determines appropriate levels of system availability based on critical system functions; provides input on system requirements to address appropriate disaster recovery and continuity of operations requirements; coaches others in the design of system architecture or system components within an enclave or enterprise (providing advice on project costs, design concepts, or design changes and input into security requirements to be included in future SOWs and other procurement documents)

Systems Security Architecture	Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
BEHAVIORAL INDICATORS	
	• Evaluates acquisition documents against existing and proposed security architectures and designs by examining the security-relevant parts of a system and interrelationships within the enterprise
4 Expert	• Applies expert knowledge of critical protocols, information assurance/ information security (IA/IS) architecture, embedded systems, network design processes, risk management, and network security architecture, including Defense-In-Depth principles, to design an organization's IT architecture • Lends expertise in systems lifecycle to the systems security design process by creating secure operating platforms for multiple functions; oversees the development of security reviews and security infrastructure analysis • Lends expertise for security protection needs (e.g., security controls) of information systems and networks when advising others on enterprise-wide security requirements to be included in complex, solution-based SOWs and other appropriate procurement and/or acquisitions documents • Blends expert knowledge in Enterprise Architecture and Defense-In-Depth principles to provide input to Security Authorization process activities and related documentation (e.g., system life-cycle support plans, concepts of operations, operational procedures and maintenance of training materials) • Validates accuracy and applicability of technical solutions to incorporate environmental conditions with business needs by analyzing these solutions against requirements and articulating them in a format that is appropriate to each audience; develops intellectual capital on enterprise; drives standardization of architectures for future use

Information Assurance (IA) Compliance	Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
BEHAVIORAL INDICATORS	
1 Basic	• Uses basic concepts of information assurance / information security (IA/IS) by applying IT security policies, principles, regulations, and vulnerabilities when assisting in monitoring and measuring system compliance • Uses IA/IS standards, practices, procedures, protocols, and standard operating procedures (SOPs) to assist in routine operations, such as verifying that network system authorization documentation is current during IT Security Authorization

Information Assurance (IA) Compliance	Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
BEHAVIORAL INDICATORS	
2 Intermediate	• Provides an accurate technical evaluation of an application, system, or network by documenting the security posture, capabilities, and vulnerabilities against relevant IA/IS controls • Maintains information system authorization and participates in the development of compliance specifications at the system and network level • Applies knowledge of IT Security Authorization requirements to monitor and evaluate a system's compliance with IT security requirements; performs validation steps, comparing actual results with expected results and identifies impact and risk • Conducts security authorization reviews for the initial installation of systems, evaluates compliance with IT security requirements, compares them with expected results and makes recommendations to system owners • Reviews systems configurations, vulnerabilities and mitigations, and monitors day-to-day compliance with policies
3 Advanced	• Analyzes Security Authorization reviews by verifying results with the organization's IA/IS requirements and confirms that the level of risk is within acceptable limits for each network • Contributes advanced skill and knowledge in information technology performance assessment, system diagnostic techniques, and existing Information Assurance Vulnerability Alerts/Information Assurance Vulnerability Management (IAVA/IAVM) • Advises others on IA/IS requirements and supports IT compliance across multiple platforms, applications, and architectures • Develops methods to monitor and measure new compliance standards by assessing current protocols and procedures and determining the most efficient course of action • Manages and tracks Security Authorization packages, reviewing authorization documents to confirm that security requirements are compliant and risk level is acceptable; makes recommendations for rejection of noncompliant packages
4 Expert	• Establishes an organization's assessment policy and reporting mechanisms for ensuring compliance with IA/IS standards, assessing them against new IT security principles, regulations, and mandates • Approves authorization packages by evaluating recommendations on Security Authorization reviews, revised or newly developed compliance specifications, and security measures, and compares them to compliance standards and overall organizational IA/IS mission and goals • Provides oversight of information systems authorization reviews, ensuring noncompliant authorization packages are rejected and those submitted for final approval are tracked • Assesses and evaluates security reviews for discrepancies or gaps and makes recommendations for new or revised security measures and Security Authorization process

Software Assurance and Security Engineering	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
BEHAVIORAL INDICATORS	
1 Basic	• Maintains software by regularly checking software for updates, testing software to ensure it works properly, making changes as required, and elevates software system abuse and misuse cases to the appropriate individuals • Consults supervisors and software engineers and compiles code and software documentation such as user guides, flow charts, system data flows, and conceptual designs to identify best software practices • Works with a mentor to design and write basic code to create applications that meet customer needs and requirements
2 Intermediate	• Designs secure software from requirements within the software development lifecycle • Maintains technology platforms by applying coding techniques within the context of the technology platform and communicating with users and senior software developers to ensure accuracy of maintenance procedures • Supports the secure design, development, testing, integration, implementation, and/or documentation of software applications, including creating and writing code for computer applications, software, or specialized utility programs • Utilizes current secure coding methodologies to develop new or modify existing code by reviewing system, determining coding needs, and communicating needs with software engineers to ensure accuracy • Performs threat and vulnerability analysis when an application or system undergoes a major change; documents findings and recommends mitigation strategies
3 Advanced	• Designs secure interface specifications between interconnected systems and validates security and integration procedures • Performs static and dynamic analysis to identify vulnerabilities in applications across databases, networks, network-based environments, and operating systems and provides remediation strategies as appropriate • Applies advanced coding techniques and diagnostics to review code and software documentation for accuracy and create secure cross-platform solutions • Enables software security automation and measurement capabilities through common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables, and common attacks on software; enhances software transparency and security diagnostic and measurement capabilities
4 Expert	• Develops and updates software development policies that meet security objectives (confidentiality, integrity, and availability) • Provides expertise in the evaluation and analyses of activities related to all phases of the secure software lifecycle from initial planning, requirements definition, design and development, through integrated system testing and operations maintenance; promotes and enables security resilience of the software • Leads the review and assessment of software system architecture, system requirements and their allocation to lower level

Software Assurance and Security Engineering	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
BEHAVIORAL INDICATORS	
	specifications; and oversees design, code and test activities, trade off studies, software independent verification and validation (IV&V) and system test and integration • Determines which coding techniques are appropriate for multi-platform implementation and oversees the implementation of security models (ensuring regulations compliance)

Systems Development	Works on the development phases of the systems development lifecycle.
BEHAVIORAL INDICATORS	
1 Basic	• Assists in systems development and information protection activities such as maintenance, troubleshooting and repair • Documents application security design features, and provides a functional description of their security implementation • Follows established procedures to assist in the installation/implementation of corrective actions to sustain operating systems functionality, usability and operability • Consults supervisors and software engineers to develop system documentation such as user guides, flow charts, system data flows, and conceptual designs
2 Intermediate	• Designs secure systems from requirements within the system development lifecycle • Conducts vulnerability scans and/or recognizes vulnerabilities in security systems in order to assess threats to computer systems/networks; drafts initial security risk profiles • Assesses the effectiveness of information protection measures used by systems, and reports findings to appropriate personnel • Participates in the design and development of system security measures that provide confidentiality, integrity, availability, authentication, non-repudiation, and protection of PII by gathering system requirements and providing recommendations to system owners and stakeholders

Systems Development	Works on the development phases of the systems development lifecycle.
BEHAVIORAL INDICATORS	
3 Advanced	• Develops detailed security design documentation for component and interface specifications in support of system design development; and develops risk migration strategies which resolve vulnerabilities and drive security changes to current systems • Evaluates the adequacy of security designs to perform risk assessments and design security countermeasures to mitigate identified risks; develops systems that provide adequate access controls, and develops countermeasures, risk mitigation strategies, • Designs secure interface specifications between interconnected systems and validates security and integration procedures
4 Expert	• Plans for the analysis, evaluation, development, coordination, implementation, deployment, support, and maintenance of multiple operating systems and networks to recommend and institute improvements, new applications, directions, and lifecycle methodologies • Develops policies that reflect system security objectives to develop and update security policies and requirements that meet the security objectives (confidentiality, integrity, and availability) of the system • Prioritizes essential system or sub-systems functions required to support essential capabilities or business functions for restoration/recovery after a system failure or during a system recovery event; develops a new system based on overall system requirements for continuity and availability • Defines and implements strategies for enterprise operating systems and application environments, and evaluates the impact of technology changes throughout the systems lifecycle to ensure compatibility with customer standards and requirements

Systems Requirements Planning	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
BEHAVIORAL INDICATORS	
1 Basic	• Conducts research to review security and organizational policies, procedures, and processes across multiple organizations; effectively communicates key findings to supervisors and managers, and provides basic input in systems requirements planning meetings • Documents and reviews requirements during meetings and takes detailed notes, clarifies information as needed, and operates the primary functions of a system

Systems Requirements Planning	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
BEHAVIORAL INDICATORS	
2 Intermediate	• Captures data and asks insightful questions to gather functional requirements from customer concerns; aligns functional requirements to standards and regulations to recommend customer-oriented solutions • Interprets customer requirements by translating customer needs into technical solutions, maps those to organizational policies, procedures, and guidelines and information security policies, and develops initial Concept of Operations (CONOPs) • Performs risk analysis, feasibility studies and/or trade-off analysis to help resolve issues and refine functional requirements and specifications
3 Advanced	• Analyzes and synthesizes customers' needs, accurately defines project scope, develops cost estimates and resources for newly acquired or modified systems implementation; ensures information security best practices are implemented in formulation of system operations requirements • Provides remediation of technical problems encountered by finding alternatives solutions • Conducts comparative analysis of customer functional requirements and available technologies, and considers IA/IS best practices to support formulation of system operations requirements
4 Expert	• Ensures customer requirements are met and resources are effectively utilized • Evaluates potential technical solutions by reviewing analyses and determining top recommended solutions that best address customer resources and expressed needs; refines CONOPs by determining the implication of the requirements and their impacts to organizational security and interoperability • Evaluates recommended functional requirements and potential technical solutions when coordinating with systems architects and developers to provide oversight in the development of design solutions • Identifies and articulates current and future agency systems needs and technical solutions that align with business needs; oversees and makes recommendations for improvement of configuration management issues

Technology Research and Development	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
BEHAVIORAL INDICATORS	
1 Basic	• Researches current technology to understand capabilities of required systems or networks and supports technology assessment and integration processes

Technology Research and Development	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
BEHAVIORAL INDICATORS	
	• Contributes basic knowledge when participating in technology assessment strategy meetings • Assists in prototype capability testing by documenting test results (e.g., meeting minutes)
2 Intermediate	• Researches current technology to understand capabilities of required system or network • Identifies vulnerabilities based on target requirements • Participates in the implementation of technology integration
3 Advanced	• Aligns prototypes to organizational strategies for customization of hardware and software that align to mission requirements and organizational technology needs • Compares and contrasts the characteristics and challenges involved in "new" systems to drive the development of integration processes • Facilitates a pre-defined transition and integration process (e.g., guides research institutions in creating a transition prototype and works with acquisition and integrators to prepare the environment for prototype integration)
4 Expert	• Ensures that measurement data collected during technology assessment is properly used in review and decision making • Leads the definition of systems integration processes and practices by lending expert knowledge of agency evaluation and validation requirements, application of vulnerabilities, and network security architecture • Oversees technology assessment and integration to ensure that the technology is fulfilling strategic business needs and the tactical dimensions of service, information, and system quality

Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).
BEHAVIORAL INDICATORS	

Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).
BEHAVIORAL INDICATORS	
1 Basic	• Executes tests by following the steps and procedures listed in a test plan and documents results in a standardized format that is appropriate for future analyses • Assists in the coordination of technical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness • Identifies the various types of tests including conformance testing, developmental testing, joint interoperability testing, operational testing, and validation testing • Performs basic and standard benchmark tests; compares current results to industry standard results and reports anomalies
2 Intermediate	• Develops general test and evaluation plans to compare current and proposed technologies; assesses test results to determine whether they match requirements specifications • Prepares documents by tailoring technical information and creates benchmark or security authorization reports; outlines key findings related to speed, risks, results and reliability, and recommends acceptance or rejection of technology for applied use • Performs Security Control Assessments on systems to validate the results of risk assessments and ensure controls in the security plan are present and operating correctly on the system; provides thorough report of the risks to the system and its data
3 Advanced	• Selects the appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; lists all steps involved for executing selected test(s) and coaches others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies • Performs joint interoperability testing on systems exchanging electronic information with systems of other services or nations, and determines whether the system is certified as interoperable based on analysis of results; provides recommendations on how to enable systems to operate effectively together • Reviews Security Control Assessment results to validate the appropriate and effective use of security services or mechanisms and certify the security assurance for a system within its respective environment; evaluates the operational impacts and residual risk against system weakness and aggregates findings
4 Expert	• Establishes test plan templates, creates schedule timeline, selects and/or gathers team members for the process • Reviews test results to validate test cases; coaches others in mitigation strategies • Leads all security evaluation efforts; ensures the accuracy and effectiveness of security certification, and security control assessments

Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).
BEHAVIORAL INDICATORS	
System Administration	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
BEHAVIORAL INDICATORS	
1 Basic	• Assists in the installation of new or modified hardware, operating systems and other software by installing cables and/or racking equipment, following establish procedures and seeking guidance from supervisors/managers • References appropriate organizational policies, works with mentors, and follows established procedures to assist in the implementation of patches and signature and application updates • Assists in the installation of server fixes, updates, and enhancements by working with mentors and following established, organizational hardware/software protocols and procedures • Assists in managing user accounts, network rights, and/or access to systems and equipment by gathering information, monitoring account databases, and periodically verifying accuracy of this information with customers
2 Intermediate	• Implements patches, provides signature and application updates and conducts periodic server maintenance that supports compatibility with agency standards and ensures continued operability • Implements access control lists and baseline system security as directed to support compatibility with agency standards • Installs cable by using hands-on skills, performs repairs on faulty server hardware, and resolves hardware/software interface and interoperability issues • Validates systems installations and integration based on knowledge of hardening documents and/or STIG requirements, connectivity diagnostics, and hardware/software configuration • Plans and coordinates the installation of new or modified hardware, operating systems, and other baseline software by maintaining a scheduling log and coordinating with customers to ensure proper/successful installation and updates • Implements baseline system security by following prescribed organizational policy and mapping these programs to organization's applicable security policies, procedures, checklists, and hardening guidelines • Manages and maintains networks in applicable settings by blending operating systems familiarity with the ability to install, configure, troubleshoot, and maintain servers to ensure their confidentiality, integrity, and availability
3 Advanced	• Determines and promulgates proper server fixes, updates, and enhancements based on a thorough assessment of user and system requirements that includes a list of issues and the solutions to fix these issues (e.g., server fixes, updates, etc.)

Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).
BEHAVIORAL INDICATORS	
	• Verifies data redundancy and system recovery by appropriate testing and identifies qualified personnel to solve any identified issues; follows the resolution to completion • Reviews and validates installation plans for new or modified hardware, operating systems, or other baseline software • Performs internal audits, reviews vulnerability scan results, and integrates server components to prioritize and schedule patches, signatures, and application updates based on vulnerability of servers • Verifies systems security baseline against application interoperability and resolve hardware/software interface interoperability problems • Effectively uses diagnostic techniques, performance tuning tools, and performance monitoring to mentor others in the general maintenance of a system • Keeps up-to-date on technological developments in server administration and draws from a variety of sources to integrate technology and develop comprehensive solutions based on user requirements • Mentors others in evaluation and analysis of functional requirements to draft hardware/software recommendations and develop customer-oriented solutions
4 Expert	• Contributes system administration expertise and hands-on experience to design access control lists and develop and oversee the documentation of system administration SOPs that ensure compatibility with agency standards and new or revised mandates • Lends expert knowledge of hardening guidelines, IT security principles, network architecture, communication protocols (e.g., TCP/IP), and configuration management to oversee the installation, implementation, configuration and ongoing optimization and support of network components (such as firewalls), while maintaining security posture • Oversees the implementation, deployment, support, and maintenance of multiple operating systems by identifying key personnel to perform tasks and resolving issues as needed • Plans, executes, and verifies data redundancy and system recovery procedures by analyzing system information for issues, creating strategies to solve these issues, and successfully executing these strategies • Oversees and directs verification and validation of installs, prioritization of patches, signatures, and application updates by identifying key personnel to perform tasks, and coaching others to resolve issues as needed • Identifies new and emerging technologies and performs comparative analysis of all applications, software and hardware (in terms of usability, cost, design, etc.) and determines which one best fulfills agency mission requirements • Oversees due diligence of validation and verification efforts to ensure a vendor's solution meets the technical requirements by

Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).
BEHAVIORAL INDICATORS	
	mapping the solution components with the requirements, making final recommendations, and articulating these recommendations to stakeholders • Identifies efficiencies and develops acquisition requirements for specialized hardware using best practices and established organization, Federal, and other guidelines and collaborates with stakeholders to further define these requirements to ensure that they are appropriate to the organization

Systems Security Analysis	Conducts the integration/testing, operations, and maintenance of systems security.
BEHAVIORAL INDICATORS	
1 Basic	• Follows established procedures to assist in the vulnerability scans and/or implementation of security measures and controls • Contributes basic skill in determining a system's security; recognizes how changes in conditions, operations or the environment can impact it • Participates in the security analysis process by applying security principles, methods (e.g., risk assessment, systems security planning, disaster recovery planning) and tools
2 Intermediate	• Determines how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes; makes recommendations that limit risk • Performs security analyses of IT activities and ensures that security measures meet security configuration guidelines, and are correctly enforced; ensures application of security patches for commercial products are integrated into systems designs for the intended operational environment • Conducts vulnerability scans and recognizes vulnerabilities in security systems to perform IA/IS testing of developed applications and/or systems • Maintains and monitors security architecture by performing security reviews, identifying security gaps, and making recommendations for the inclusion into risk mitigation strategies • Participates in the evaluation of information systems by assisting in the development of security plans

3 Advanced	• Applies advanced skill in developing and applying security system access controls and designing security risk countermeasures to mitigate/correct security deficiencies during security control assessment and/or identify residual risk • Monitors and oversees that the system security requirements and IA/IS countermeasures identified in the system security plans are incorporated into the systems development lifecycle process; thoroughly reviews work detecting errors and inaccuracies • Plans, executes, and verifies that recovery and continuity plans are executable in the operational environment by analyzing system information for issues, creating strategies to resolve these issues, and successfully executing these strategies
4 Expert	• Designs plans and implementation strategies by including measures, testing procedures, and evaluation guidelines to ensure consistency across the organization for information systems security plans • Develops procedures and policies for system security plans throughout the organization using best practices and established guidelines; further defines requirements to ensure they are appropriate for the organization • Formulates and implements improvement strategies by keeping up with organizational trends and emerging technologies with regard to the security posture of systems and selecting the best methods to comply with security controls • Develops risk management framework, and identifies and reports impact of residual risk on the organizational mission, and provides recommendations to organizational leadership

Customer Service and Technical Support	Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
BEHAVIORAL INDICATORS	
1 Basic	• Responds to customer-reported issues by reviewing issue details and consulting applicable source material • Follows up with and tracks customer-reported system issues by using established guidelines and procedures; gathers information on reported system incidents from customers to support recovery and continuity of operations; seeks appropriate technical experts to follow up with the customer and provide updates on resolution efforts • Assists with account maintenance and monitors databases and account logs • Assists with the installation and configuration of hardware, operating systems, and other baseline software for system users by resourcing established protocols (e.g., handbooks, manuals, guidelines), seeking guidance, and following established protocols and SOPs

Customer Service and Technical Support	Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
BEHAVIORAL INDICATORS	
2 Intermediate	• Plans and coordinates the installation of approved requirements for hardware, operating systems, and other baseline software by maintaining a scheduling log and coordinating with customers to ensure proper/successful installation and updates • Diagnoses problems and devises customer oriented solutions • Reviews change requests to determine validity and feasibility and collaborates with users to make recommendations for appropriate changes to a system • Troubleshoots system hardware and software and assesses systems for shortcomings against functional requirements to troubleshoot system hardware and software errors; assesses problems and resources appropriate handbooks, manuals, and guidelines • Monitors client-level computer system performance, and applies troubleshooting skills to determine necessary repairs • Provides approval/disapproval on role-based access/content/active channel requests by reviewing whether requests comply with organizational standards and procedures
3 Advanced	• Conducts root cause analysis to create enterprise-wide recommendations and improvement strategies • Analyzes trends around customer requirements and inquiries to determine when training may be required; conducts training on how to use various tools and products using best practices • Assesses systems against business requirements, functionality, and standards to provide guidance on configuring change requests through training and written guidance (e.g. SOPs, manuals) • Assesses systems for shortcomings related to business requirements, functionality, or policy compliance, and develops and documents mitigation steps and procedures (e.g. SOPs on how to use CND tools) • Troubleshoots, diagnoses, and resolves customer-reported system issues or incidents by analyzing them for key themes; coaches others in troubleshooting, diagnosing, and resolving customer issues, events or incidents • Analyzes events or incident data from various sources to identify emerging trends and vulnerabilities, and synthesizes information into findings and recommendations reports, escalating as appropriate

Customer Service and Technical Support	Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
BEHAVIORAL INDICATORS	
4 Expert	• Manages allocation of IT resources based on organization's rules, regulations, and stakeholders' immediate and projected IT needs • Reviews and approves recommendations for possible improvements and upgrades by ensuring they directly relate to the organization's mission and business needs • Develops strategic plans and initiatives in support of organization's mission and requirements

Data Administration	Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.
BEHAVIORAL INDICATORS	
1 Basic	• Performs basic retrieve and commit data processing by leveraging knowledge of basic database models • Assists in gathering data requirements and specifications that will support an organization's ability to plan for anticipated changes in data capacity requirements by using basic database modeling concepts • Manipulates data by following established processes and protocols; identifies issues and seeks guidance from database administrators, supervisors, or managers to verify data manipulation
2 Intermediate	• Identifies system requirements (e.g., data requirements and specifications) to determine feasibility of an installation; successfully installs applications • Reviews status of software, and reports findings related to anticipated changes in data capacity, and maintains assured message delivery systems and replication services • Assists in the indexing, tuning, and performing of partition splits; maintains systems by performing system upgrades, applying patches, and considering architectural placement
3 Advanced	• Designs and develops databases and applies analytical and database modeling skills to determine how to tailor these to requirements, while coaching others in these areas • Evaluates backup and retention procedures by collaborating with leadership to determine and agree upon priority and criticality of backup and retention procedures • Develops and oversees the implementation of data mining and data warehousing programs; develops processes to accurately capture system data

	• Develops policies on servers to run data backup on established schedules by aligning organizational policy and server capabilities to help create tailored and appropriate polices
4 Expert	• Studies new database technologies and architectures to evaluate backup and retention procedures; synthesizes evaluation and collaborates with other leaders to determine priority and criticality of backup and retention procedures • Oversees the evaluation, selection, and integration of database management systems by creating policies and procedures for the processes and coaching others on how to mitigate issues that occur • Approves technical approach and organizational standards for database development and administration

Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
BEHAVIORAL INDICATORS	
1 Basic	• Performs the indexing/cataloging, storage, and access of organizational documents by routinely testing the system to ensure it is working properly; provides users with directions on how to use the system • Draws from basic understanding of knowledge management technologies to describe the role of technology in converting data and information into organizational knowledge and shares best practices for utilization with stakeholders • Performs basic functions to construct access paths to suites of information (e.g., link pages) and provides the links to end users • Gathers requirements for end-user needs, based on appropriate knowledge of repository technology, for a given application environment and facilitates access to intellectual capital and information content
2 Intermediate	• Implements appropriate knowledge management repositories and technologies for a given environment while applying IA/IS principles, policies, and procedures • Administers the indexing/cataloguing, storage, and access of organizational data via data mining and knowledge mapping • Uses tools (e.g., wikis, social networking, blog) to implement knowledge management systems and support a culture of knowledge sharing and collaboration • Matches the appropriate knowledge repository technology for a given application or environment to construct access paths to suites of information (e.g., link pages) and facilitate access for end users; provides recommendations on data structures and databases that ensure correct quality production of reports/management information • Identifies opportunities where existing information can be transferred into knowledge and made discoverable through automated means; applies the four levels of knowledge management (data, information, knowledge and wisdom,) to support the strategic goals set forth by the organization • Strengthens links between knowledge sharing and IT systems

Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
BEHAVIORAL INDICATORS	
3 Advanced	• Aligns agency information flows to its structure and processes and synthesizes this information so decision makers and users acquire the desired information at the right time • Recommends, designs, builds, implements, and maintains knowledge management systems, that provide end-users access to the organization's intellectual capital in accordance with IA/IS policy by obtaining key information such as number of users, type of information, and location of storing information • Develops and implements an integrated knowledge management process by exploring and analyzing the role that organizational culture and sponsorship play and incorporating key IA/IS concepts into the strategic knowledge management implementation plan
4 Expert	• Evaluates control procedures and oversees design, development and implementation of core IT-based knowledge management systems; works within budget to ensure appropriate tools are available to support these systems • Works across organizational boundaries and develops cross-functional teams to develop a lexicon for overarching, interagency knowledge management solutions • Evaluates a variety of organizational approaches (policies, budget, assessment, rewards) that can be used to institutionalize knowledge management processes successfully and selects the best method for creating, overseeing and implementing an agency-level knowledge management solution • Creates policy statements on knowledge management systems to articulate a vision of its strategic importance to the organization including IA/IS policy

Network Services	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
BEHAVIORAL INDICATORS	
1 Basic	• Follows prescribed SOPs to conduct functional and connectivity testing to ensure continuing operability • Performs repairs on faulty server hardware by collaborating with managers or mentors to solve hardware problems • Installs new or modified network infrastructure device operating system software (e.g., IOS, firmware, etc.) and installs or replaces network hubs, routers, and switches by using established protocols and procedure, with supervision or guidance
2	• Configures and tests computer hardware, networking software, and operating system software and monitors internal and

Network Services	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
BEHAVIORAL INDICATORS	
Intermediate	external data sources • Performs system administration through the use of tuning tools, diagnostic tools, fault identification techniques, and software configuration and optimization protocols • Protects, defends and restores network services and capabilities by maintaining and administering computer networks and related computing environments (such as computer hardware, software, applications software, and configurations) • Manages and maintains networks in applicable settings by blending familiarity with multiple operating systems with the ability to install, configure, troubleshoot, and maintain server configurations to ensure their confidentiality, integrity, and availability
3 Advanced	• Verifies and validates network configuration by thoroughly reviewing work and using technical knowledge to detect errors and inaccuracies • Implements and supports multi-vendor, multi-product hardware infrastructure and/or diverse hardware platforms by designing implementation plans and resolving detected problems, including interoperability • Verifies and ensures systems security baseline supports interoperability • Resolves hardware/software interface interoperability problems and ensures user access to these systems
4 Expert	• Develops comprehensive, enterprise-wide solutions based on user requirements, including those for network architecture and infrastructure • Integrates technology, security, and operational knowledge to develop network strategies • Oversees the installation, implementation, configuration, and ongoing optimization and support of network services and components (network hubs, routers, switches, protocols, tunneling, IOS, firmware, etc.) • Develops and oversees the implementation of network and backup and recovery procedures, design procedures, and test procedures, and maintains network quality standards across an enterprise

Computer Network Defense (CND) Analysis	Use defense measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

BEHAVIORAL INDICATORS	
1 Basic	• Gains situational awareness by collecting network security sensor information to track network events and activities and report all incidents to appropriate personnel • Conducts data calls for information from other components for technical solution review by sending out mass correspondence, fielding feedback, and collecting information in an organized and accurate format • Follows prescribed, SOPs to monitor signatures and access control mechanisms that can be implemented on security systems; uses prevention and detection technologies and log checks to monitor networks and operating systems to identify anomalous network behavior or traffic patterns against steady-state, baseline network activity • Supports network administrators in the active defense of the enterprise level network controls through protective technologies
2 Intermediate	• Hardens, configures, diagnoses, troubleshoots and/or resolves hardware, software, or other network and system problems using network security knowledge • Maintains and administers computer networks and related computing environments to protect, defend, and restore network services and capabilities • Participates in the analysis, evaluation, development, coordination, and dissemination of security tools and procedures to eliminate system vulnerabilities and threats • Monitors external data sources to maintain current CND threat condition and determine which security issues may have an impact on the network; assists in the development of signatures and thresholds that trigger network based event alerts and develops draft mitigation recommendations
3 Advanced	• Analyzes network alerts from various sources and synthesizes this information to identify new malicious activity within monitored and develops network and/or network mitigation strategies • Oversees notifications for CND managers, CND incident responders, and other CND-Service Provider team members of suspected or confirmed CND incidents • Designs, configures, and tests computer hardware, networking software, and operating system software, and determines which security issues may impact the network • Develops certification documentation and reviews and tracks audit findings to determine risk levels and recommends changes to the organization's IA/IS standards and procedures
4 Expert	• Reviews event correlations; validates and approves recommended mitigation efforts based on analysis of network alerts • Oversees and coaches others in network discovery, hardening, configuration, diagnostics, and enterprise-wide mitigation strategies • Ensures system requirements identified in the system security plan are incorporated into the systems development lifecycle process by comparing current authorized systems against established lifecycle processes

Computer Network Defense (CND) Analysis	Use defense measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
BEHAVIORAL INDICATORS	
	• In coordination with senior leadership, analyzes, defines, develops, and implements enterprise-wide encryption strategies; designs and oversees the construction of signatures and thresholds that trigger network based event alerts; and develops procedures and policies for evaluating, coordinating, and disseminating security tools and strategies for security planning and testing

Computer Network Defense (CND) Infrastructure Support	Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.
BEHAVIORAL INDICATORS	
1 Basic	• Supports network administrators in the active defense of network controls through ACL block requests • Follows prescribed SOPs to create and edit network access accounts by accurately gathering user information (e.g., username.) • Makes edits to network access control lists or firewalls; uses SOPs or established, prescribed testing protocols to assess rules/signatures, access controls, and configurations to report suspected anomalies
2 Intermediate	• Identifies potential conflicts with the implementation of CND tools within the CND service provider area of responsibility; manages and administers the updating of rules and signatures); mitigates these conflicts and protects the system through tool/signature testing and optimization • Applies tuning tools, diagnostic tools, fault identification techniques, and software configuration and optimization protocols to perform system administration on specialized CND applications and systems (e.g., anti-virus, Audit/Remediation, or VPN devices includes installation, configuration, maintenance, and backup/restore • Implements security authorization requirements for specialized CND systems within the enterprise, and documents and maintains records for them

Computer Network Defense (CND) Infrastructure Support	Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.
BEHAVIORAL INDICATORS	
3 Advanced	• Applies host/network access controls to oversee changes to network access control lists on specialized CND systems (e.g., intrusion detection prevention systems) and coach others in these areas • Leads others in the administration of CND test beds and the evaluation of new CND applications, rules/signatures, access controls to build and install specialized hardware/software; oversees its deployment at remote and local sites
4 Expert	• Develops acquisition requirements for specialized CND hardware using best practices and established guidelines and collaborates to further define these requirements to ensure they are appropriate to the organization; coaches others in these activities • Assesses network security controls; devises strategies for overseeing the implementation of Security Authorization requirements for specialized CND systems within the enterprise; and ensures documentation and records are maintained for these systems

Incident Response	Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
BEHAVIORAL INDICATORS	
1 Basic	• Maintains awareness and reports alerts from various sources within the enterprise to management; requests digital media (e.g., thumb drives, flash drives, and hard drives), and provides it to incident response/field support teams for further analysis • Performs internal and external research with guidance, searching for similar or related network events or incidents in tracking tools (e.g., Remedy) • Maintains a status (situational awareness) of security sensor events and incidents to provide real-time status reporting on systems, controls and resources • Uses an event as an opportunity to observe and understand the formal protocols and procedures for an incident investigation • With guidance, queries proxy logs to assist CND personnel and assist with mitigation of incidents as directed
2	• Maintains and administers computer networks and/or related computing environments, including computer hardware,

Incident Response	Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
BEHAVIORAL INDICATORS	
Intermediate	software, applications software and all configurations to protect, defend and restore cyber related services and capabilities • Performs analysis of log files from a variety of sources to identify threats and assists in the development of signatures that trigger network based event alerts and conducts backup and recovery to prevent events and incidents • Performs incident triage by determining scope, urgency, and potential impact, and collaborating with incident responders to mitigate the incident • Tracks and documents cyber related incidents from initial detection through final resolution by following established procedures and protocols; verifies that incidents have reached final resolution prior to completing tracking documentation
3 Advanced	• Analyzes cyber related alerts from various sources and performs log analysis (e.g. firewall logs and intrusion detection system logs) and synthesizes this information to identify abnormal activity • Collects and analyzes intrusion artifacts (e.g., source code and security event logs) to troubleshoot, diagnose, and mitigate cyber related incidents • Reviews and analyzes a cyber related incident and develops cyber related guidance and reports on incident findings for appropriate constituencies • Designs and oversees the construction of signatures that trigger network based event alerts • Reverse engineer and/or conducts root-cause analysis
4 Expert	• Develops enterprise-wide (to include corporate, federal department, public service agency) mitigation strategies for identified or abnormal cyber related activities • Oversees and coaches others in network mapping, hardening, configuration, diagnostics, and mitigation strategies • Correlates incident data to identify exploited vulnerabilities; makes recommendations that enable expeditious remediation and provides enterprise-wide strategies to prevent future occurrences • Reviews and validates the construction of signatures that trigger network based event alerts

Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
BEHAVIORAL INDICATORS	
1	• Assists in developing security audit reports by gathering/recording data during audit activities

Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
BEHAVIORAL INDICATORS	
Basic	• Demonstrates knowledge of basic cyber related configuration and topology when assisting with network security control testing • Works with a mentor to identify weaknesses by testing management, operational, and technical security controls for vulnerabilities of a cyber related components against general guidelines and polices; provides input to simple vulnerability assessment activities
2 Intermediate	• Uses penetration testing tools to conduct authorized penetration testing to determine the effectiveness of security controls and report findings • Conducts vulnerability scans and recognizes exploitable vulnerabilities in security systems when preparing audit reports • Uses vulnerability assessment tools to perform system audits on management, operational, and technical security controls to identify gaps, determine risks and recommend mitigation procedures in accordance with established guidelines
3 Advanced	• Interprets organizational security guidelines and evaluates and provides recommendations on audit activities • Determines deviations from acceptable configurations and develops appropriate mitigations and countermeasures within security designs (e.g., enterprise architecture, firewalls, routers, VPN, and security technologies) • Ensures auditing activities accurately reflect the auditing process by reviewing current operations and mapping operational processes to appropriate guidelines • Reviews threat and vulnerability assessment findings to quantify and prioritize vulnerabilities in a system; acts to either mitigate or accept known risks and makes recommendations to senior management for corrective measures (e.g., residual risk) • Shares best practices for adherence to established guidelines when reviewing and validating audit reports for quality and comprehensive depiction of security auditing functions • Performs continuous monitoring to analyze near real-time vulnerabilities and anomalies; interprets security and privacy related dashboards, and aggregates data collected to inform senior management
4 Expert	• Conducts research on continuous improvement and presents and prepares publications on security auditing functions to enhance Vulnerability Assessment Management activities within the organization • Establishes organizational/agency criteria and testing methodologies for conducting vulnerability assessments • Assesses vulnerability assessment and audit team performance on evaluation engagements and ensures alignment of evaluation process with critical infrastructure goals and cybersecurity missions • Leads and influences communities of interest regarding corrective measures

Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
BEHAVIORAL INDICATORS	
	• Provides analyses on complex program-related IT issues or problems and oversees the areas where new vulnerability assessment techniques must be developed, identified, and evaluated to provide solutions that align to other agency cyber operations and mission plans

Digital Forensics	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
BEHAVIORAL INDICATORS	
1 Basic	• Assists team members in imaging digital media; under direct guidance and coaching, works to define the structure and locate critical items in multiple file systems • Uses government approved standards and technologies to create forensic artifact(s); conducts preliminary analysis by tracing an activity to its source and documents findings, and provides input into forensic reports • Utilizes various government and commercial resources to research known malware, define its characteristics, and report findings and mitigation recommendations to appropriate personnel • Uses prescribed methods and materials to provide basic incident response and/or technical assistance to situational response teams (e.g., scanning digital media for viruses) • Follows and understands the proper procedures to preserve chain of custody for legal review
2 Intermediate	• Acquires and/or collects forensic artifacts on potential or confirmed systems that have been compromised or misused to facilitate assessment of cause and effect; captures forensic images and uses industry standard forensic investigative tools to assesses current state of digital artifacts; drafts preliminary forensic reports • Uses current hashing algorithms to validate forensic images; diagrams networks and images servers to support digital forensics operations • Utilizes a variety of industry standard tools and techniques to collect a system's current state data and catalog, document, extract, collect, and preserve information • Uses dynamic analysis to identify network intrusions and network monitoring tools to capture real-time traffic spawned by any running malicious code; identifies internet activity that is triggered by malware; identifies network/host-based characteristics and assists in drafting recommendations to mitigate malware effects

Digital Forensics	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
BEHAVIORAL INDICATORS	
3 Advanced	• Reviews collected data and forensic analyses and/or preliminary forensic reports to determine the cause and effect of probable incidents and establish mitigation strategies to prevent future incidents • Identifies activities leading up to and including initial intrusion vector using an approved list of tools; identifies artifacts related to the infection; coaches forensics teams in post-activities and final reporting and writes detailed reports that summarize this information and presents to senior leadership • Uses suite of network monitoring tools to identify vulnerability exploitation and suspected vector; attempts identification and mitigation of all malware and identifies all registry key and file changes
4 Expert	• Enhances forensic analysis efforts by maintaining a robust digital media analysis laboratory that permits in-depth analysis of images and individual files and artifacts • Oversees forensic analysis by mentoring and providing guidance to others through data collection and analysis and verifying analysis outcomes and reports • Lends forensic and investigative expertise and forensics knowledge to establish criteria for conducting digital forensic investigation activities; coordinates and delegates activities of forensic teams • Provides subject matter expert testimony when required • De-obfuscates, re-engineers and analyzes malicious code to plan and execute digital forensic investigation

Investigation	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
BEHAVIORAL INDICATORS	
1 Basic	• Identifies conditions and circumstances required to open a case (e.g. criminal, espionage, foreign intelligence gathering, and/or auditing) and assists in triaging residential scenes by cataloging any devices that are designed to or are able to store digital media • Uses industry standard tools to develop forensic artifacts • Under direct supervision and guidance, follows preliminary leads using various methods (e.g., tracing an activity to a source address, identifying locations of interest, and acquiring and serving search warrant) • Accesses and gathers evidence from electronic devices and file systems using forensic tools and basic knowledge of network mapping methods, systems, and encryption

Investigation	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
BEHAVIORAL INDICATORS	
	• Follows established protocols to support computer network defense personnel in investigative activities by sending data calls, gathering real-time information and reporting on information regarding computer generated threats
2 Intermediate	• Participates in digital forensics operations of large organizations by diagraming networks and imaging servers • Participates in criminal trial proceedings by appearing as a witness, answering questions from counsel, and articulating findings, methods, and evidence in a manner the audience can understand • Accesses, assesses, and gathers evidence from electronic devices using various forensics tools • Establishes and maintains relationships with incident response teams and other groups to support computer network defense activities (e.g. conducting investigation surveillance and counter surveillance)
3 Advanced	• Establishes criteria for conducting investigation activities and coordinates preliminary investigation activities of others to identify locations of interest and acquire and serve search warrants • Recognizes vulnerabilities and develops and executes risk management processes, including steps and methods for assessing risk in security systems to analyze cyber threats; conducts trend analysis and oversees the implementation of preventative measures and counterattacks • Coordinates triage activities to ensure forensic team members are effectively assessing large data sets and overall risk/liability to expedite incident containment and response
4 Expert	• Directs the triage of incident site activities for forensics teams that are interacting with large data sets, different operating systems, and complex networks and assesses overall risk/liability • Oversees and develops agency protocols and SOPs for investigation interviews, interrogation, and surveillance that facilitates cyber incident response team's ability to identify conditions and circumstances that require the opening of a criminal case • Coordinates and delegates activities of forensic team members and provides subject matter expertise and assistance when necessary • Establishes and maintains relationships (both internally and externally) with incident response personnel (e.g., legal department, law enforcement agencies, vendors, public relations professionals, and other federal entities) to support investigative processes • Dictates techniques tactics and procedures (TTP) for chain of custody

Collection Operations	Executes collection using appropriate collection strategies and within the priorities established through the collection management process.
BEHAVIORAL INDICATORS	
1 Basic	• Actively collects network information to report tactical information and reporting data, provide timely indicators and warnings to CND personnel, and assist in documenting exploitations that could compromise the confidentiality, integrity, and availability of information and/or networked information systems • Conducts data calls for information from other components for technical solution review by sending out mass correspondence, fielding feedback, and collecting information in an organized format that is consistent with the collection management process • Identifies and tracks threats in support of event correlation activities by gathering information from internal sources to gain situational awareness
2 Intermediate	• Uses dynamic analysis to identify an intrusion, confirm what is known about an intrusion and discover new information • Uses a variety of tools and techniques to scan systems (e.g. work stations and servers (to include various implementations of RAID), document and collect system state information (running processes, network connections, etc.), and document, collect, and preserve digital media in the form of forensic images • Performs incident triage to include determining scope, urgency, and potential impact to make recommendations that enable expeditious remediation; provides initial drafts of technical documents, incident reports, and findings from computer examinations, summaries, and other situational awareness information • Examines malicious software, suspicious network activities, and/or non-authorized presence in the network to assess the nature of the threat, and secure and monitor firewall configurations • Monitors external data sources to maintain current CND threat condition and determine which security issues may have an impact on the network
3 Advanced	• Collects, processes, preserves, analyzes, and presents computer-related evidence to support CND operations and coordinates; writes in-depth reports of findings; and/or reviews peer or junior level analysts' reports • Evaluates external threats and vulnerabilities against the operation and environment to facilitate and develop data-gathering methods that control and minimize risk • In order to enhance ongoing assessment and situational capabilities, keeps abreast of specialized CND test tools and selects the appropriate technical tests, network and vulnerability scan tools, and/or pen testing tools based on review of requirements • Monitors external data sources (e.g., CND vendor sites, Computer Emergency Response Team current operating pictures, SANS, Security Focus), captures and analyzes information related to suspected incidents, correlates threat data, and

Collection Operations	Executes collection using appropriate collection strategies and within the priorities established through the collection management process.
BEHAVIORAL INDICATORS	
	determines likelihood and impact on the enterprise • Prepares and/or satisfies data collection requirements, evaluates reporting from collectors in response to requirements, and provides guidance/feedback to field elements that support analytical efforts • Performs event correlations, trend and pattern analysis and makes correlations to gain situational awareness and determine likelihood and impact of an observed attack or project future scenarios; validates and approves recommended mitigation efforts
4 Expert	• Establishes criteria for conducting investigation activities and coordinates preliminary investigation activities of others in order to identify locations of interest and acquire and serve search warrants • Oversees and develops agency protocols and SOPs for investigation interviews, interrogation, and surveillance that facilitate forensic agents' ability to identify conditions and circumstances that require the opening of criminal cases • Establishes and maintains relationships (both internally and externally) with incident response personnel to include the legal department, law enforcement agencies, vendors, public relations professionals, and other federal entities to support investigative processes, surveillance, counter-surveillance and detection • Develops advanced technologies for processing and integrating data from a variety of sources, such as radar, electro-optic video sensors, and related, unstructured textual data to support timely and effective decision making • Communicates, coordinates, and collaborates with a wide variety of inter-organizational and external stakeholders (e.g. legal department, other federal entities, forensic team members, etc.) to write analytic reports, assessments, and summaries of activities occurring in the cyber domain

Cyber Operations Planning	Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
BEHAVIORAL INDICATORS	
1 Basic	• Gathers and provides information to senior stakeholders in support of cyber operations planning activities • Makes updates to SOPs, reference manuals, and information sources and articulates basic cyber operations concepts to others • Supports incident management/ response (IMIR) activities by reporting alerts and notifying and assisting senior stakeholders in managing cyber-related events or incidents

Cyber Operations Planning	Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
BEHAVIORAL INDICATORS	
2 Intermediate	• Keeps abreast of emerging cyber technologies and gathers information on data security policies, and legal and regulatory requirements to make informed recommendations toward the development of detailed cyber operations plans • Reviews an agency's cybersecurity protocols and operating procedures and makes recommendations for improving its cyber operations plan • Identifies compliance gaps and collaborates with colleagues and leadership to identify gaps in processes and update cyber operation policies as necessary
3 Advanced	• Guides others in achieving their strategic cybersecurity goals; develops policies that incorporate compliance, oversight, education, awareness, performance measures, and metrics into the overarching cyber operations plan; aligns cyber operation plans to other agency mission plans to organize information services into a common solution for the Federal Government • Performs event trend analysis by correlating event data to identify specific vulnerabilities, and provides recommendations for preventing and/or mitigating the threat of future event(s) • Advises others in the oversight of cyberspace operations management and coaches them in the development of tools to track milestones, tasks, and resources required to support cyber missions
4 Expert	• Analyzes data security policies, and legal and regulatory requirements for the purposes of developing detailed cyber operations plans and defining measurable criteria and metrics to monitor success • Oversees the development of cyber operation plans that align to other agency mission plans

Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
BEHAVIORAL INDICATORS	
1 Basic	• Works with a mentor to perform network monitoring to maintain situational awareness of security sensor events and incidents, and provide real-time status reporting on systems, controls, and resources • Actively collects network configuration information to assist network defense analysts in documenting exploitation of software configurations of information technology systems, as well as activities which could compromise the confidentiality, integrity and availability of information, and/or networked information systems

Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
BEHAVIORAL INDICATORS	
	• Assists in the production of briefings and written activity reports that support cyber operations and tactical requirements • Recognizes and adheres to information assurance/security policies and procedures, and interprets guidelines and capabilities with supervisor or peer guidance
2 Intermediate	• Uses packet capture tools (e.g., WireShark, dsniffer, NetStumbler, tcpdump) to examine data from live networks and identify potential anomalies; distinguishes false positives; makes recommendations regarding threat levels and further investigation • Participates in the analysis, evaluation, development, coordination and dissemination of security tools and procedures that support management and monitoring of cyber operations • Develops estimates and projections of possible malicious activities and cybersecurity threats by applying intelligence, threat analysis, forecasting and analytical methodologies to cyber threat and security issues • Distinguishes, researches and articulates all-source cyber computer network operations (CNO) national military intelligence studies, plans and/or products using the Intelligence Community Directory (ICDs)
3 Advanced	• Evaluates all-source intelligence and open source information, and/or evaluates collection system solutions to support the intelligence production process to provide recommendations to stakeholders • Conducts all-source research, makes correlations and performs trend and pattern analysis; uses appropriate tools and tactics, and performs procedural tactical, nodal and link analysis to identify, assess and document projections and estimates of future technical cyber threat scenarios • Enables software security automation and measurement capabilities through the use of common indexing and reporting capabilities for malware, exploitable software weaknesses, vulnerabilities, cyber observables and common attacks; enhances software transparency and security diagnostic and measurement capabilities
4 Expert	• Leads in the analysis, evaluation, development, coordination and dissemination of security tools to eliminate system vulnerabilities and manage, monitor and/or execute large-scale cyber operations in response to national and tactical requirements • Defines and implements strategies for security planning and testing, and directs, administers and monitors CND efforts across multiple operations • Communicates, coordinates and collaborates with a wide variety of inter-organizational and external stakeholders and

Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
BEHAVIORAL INDICATORS	
	leaders to write analytic reports, assessments and summaries of activities occurring in the cyber domain and provides input into national-level cyber-operations improvement plans • Evaluates, interprets and integrates all sources of information to include data that would be considered network intelligence to produce assessments in line with policy and guidance

All Source Intelligence	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
BEHAVIORAL INDICATORS	
1 Basic	• Leverages knowledge of the Intelligence Community (IC) including the interaction and responsibilities of major components (e.g., DHS, DIA, NSA, etc.) to gather data in support of production of briefings and written activity reports • Conducts information searches in efforts to identify potential threats and effectively communicate key findings with supervisors and managers • Actively collects network configuration information to assist in documenting exploitation of software configurations of information technology systems, as well as activities which could compromise the confidentiality, integrity, and availability of information and/or networked information systems
2 Intermediate	• Reviews multiple sources of intelligence to identify potential threats and summarizes them for key stakeholders, and provides recommendations within the customer's mission requirement and needs • Provides all-source intelligence analysis of cyber activities to identify entities of interest, methods, motives, and capabilities and informs appropriate supervisors • Analyzes, assesses and reports threat intelligence based on CNE/CNA/CNO methodologies and industry-standard and organizationally accepted analysis principles and methods
3 Advanced	• Evaluates all-source intelligence and open source information and/or collection systems solutions to support the production of intelligence products that identify adversarial tools, techniques, and methods of operation; assesses whether it can be turned to advantage • Analyzes threat information from multiple sources, disciplines, and agencies across the intelligence community to synthesize information, build context around threats, and derive possible implications; develops comprehensive mission

All Source Intelligence	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
BEHAVIORAL INDICATORS	
	reports based on a variety of sources for senior leadership and stakeholder review and discrimination • Uses appropriate tools and tactics, and performs procedural tactical, nodal, and link analysis to identify, assess, and document projections and estimates of future technical cyber threat scenarios • Coordinates combined Counter-Intelligence and CNA/Computer Network Environment/Computer Network Defense efforts by keeping up to date on all efforts and identifying potential areas of conflict
4 Expert	• Develops advanced technologies for processing and integrating data from a variety of sources, such as radar, electro-optic video sensors, and related, unstructured textual data to support timely and effective decision making • Analyzes and synthesizes information with other relevant data sources to develop a common operational picture of criminal and foreign threats to information infrastructure • Fuses computer network attack analyses with criminal and counterintelligence investigations and operations and promotes joint operations and shares best practices with other members of the intelligence community • Analyzes mission reports from various data sources and synthesizes this information to identify known malicious activity, develop mitigation strategies, and outline potential contextual implications • Evaluates, interprets, and integrates all sources of information to include data that would be considered network intelligence to produce assessments in line with policy and guidance

Threat Analysis	Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
BEHAVIORAL INDICATORS	
1 Basic	• With guidance and supervision, uses common digital forensics tools and techniques to collect, document, and report intelligence information derived from various intelligence sources • Assists senior leadership in preparing multi-disciplined intelligence and law enforcement reports to document analysis • Collects intelligence and actively identifies cyber threats and counterintelligence information with supervisor using front-end collection systems, including network traffic collection, filtering, and selection • Follows industry-standards and organizationally accepted analysis principles and methods to assist in determining threat targets based on collected data
2 Intermediate	• Analyzes, assesses and reports threat intelligence using CNE/CNA/CNO methodologies, industry-standards and organizationally accepted analysis principles and methods

Threat Analysis	Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
BEHAVIORAL INDICATORS	
	• Translates, tracks, and prioritizes information needs and collection requirements across the extended enterprise to organize topics and key points according to guidance for intelligence writing • Analyzes computer systems activity and report findings to leadership using operating systems and network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services
3 Advanced	• Uses common digital forensics tools and techniques to assess and/or validate criminal or Counter-Intelligence evidence to ensure accuracy of reporting • Supports the development of intelligence products used to identify adversarial tools, techniques, and methods of operation and assesses whether it can be turned around. • Coordinates combined Counter-Intelligence and CNA/Computer Network Environment/Computer Network Defense efforts by keeping up to date on all efforts and identifying potential areas of conflict; mitigates any identified gaps or interference issues and delegates the responsibility to the appropriate personnel
4 Expert	• Keeps current on evolving and emerging technologies that may involve multi-disciplined intelligence and/or evoke new threats and interfaces with other organizations to maintain situational awareness, stay ahead of future threats and leverage best practices • Applies expert knowledge of the nexus between Cyber Counter-Intelligence and other Intelligence operations (i.e., How/ Where/ When Cyber Counter-Intelligence fits in, etc.) • Analyzes and synthesizes information with other relevant data sources to develop a common operational picture of criminal and foreign threats to information infrastructure • Fuses computer network attack analyses with criminal and counterintelligence investigations and operations ,promotes joint operations, and shares best practices with other members of the intelligence community

Exploitation Analysis	Analyzes collected information to identify vulnerabilities and potential for exploitation.
BEHAVIORAL INDICATORS	
1 Basic	• Works with a mentor to identify weaknesses by testing management, operational, and technical security controls for vulnerabilities of a network against general guidelines and polices and provide input to simple vulnerability and exploitation analysis activities
2	• Uses a suite of network monitoring tools to identify vulnerability exploitation and suspected vector; attempts identification

Exploitation Analysis	Analyzes collected information to identify vulnerabilities and potential for exploitation.
BEHAVIORAL INDICATORS	
Intermediate	and mitigation of all malware; and identifies registry key and Windows file changes • Conducts assessments of threats and vulnerabilities, and aggregates and synthesizes findings to create metrics of vulnerabilities, findings, and recommendations to develop audit reports for senior leadership review • Conducts intelligence analysis to assess intrusion signatures, tactics, techniques and procedures associated with preparation for and execution of cyber attacks • Researches hackers, hacker techniques, vulnerabilities, and exploits, and aggregates findings into detailed intelligence reports and briefings
3 Advanced	• Correlates incident data to identify exploited vulnerabilities and makes recommendations that enable expeditious remediation • Analyzes network alerts from various sources, to include firewall logs and intrusion detection system logs and synthesizes this information to identify known malicious activity within monitored networks
4 Expert	• Develops advanced technologies for processing and integrating data from a variety of sources, such as radar, electro-optic video sensors, and related, unstructured textual data to support timely and effective decision making. • Oversees the development of efficient data and network management software systems to transform high-volume data streams into tactically useful information and provides guidance where new techniques or solutions must be developed • Correlates incident data to identify exploited vulnerabilities and makes recommendations that enable expeditious remediation; provides enterprise-wide strategies to prevent future occurrences • Participates in regular Intelligence Community (IC), DHS, and DOD collaboration meetings to report on and coordinate remediation of cyber threats and contribute expertise on ongoing cyber threat assessment across Federal Government

Targets	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
BEHAVIORAL INDICATORS	
1 Basic	• With direct guidance, and supervision, gathers information from threat assessments and all-source intelligence reports to assist in the development of mission reports
2 Intermediate	• Identifies and analyzes potential emerging threats and generates initial threat assessment reports using knowledge of politics, history, societal trends, and underlying principles and background

Targets	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
BEHAVIORAL INDICATORS	
3 Advanced	• Uses information gathering results to create or enhance the quality of deliverables and informational products aimed to mitigate vulnerabilities and outline potential emerging threats; informs inquiring organization(s) of existing threats based on threat assessment scores
4 Expert	• Ensures identified threats and recommendations reflect Federal security goals in cybersecurity practice and support infrastructure protection via cybersecurity capacity and capability building

Legal Advice and Advocacy	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
BEHAVIORAL INDICATORS	
1 Basic	• Conducts legal research, summarizes findings, and contributes to sections of policy drafts related to U.S. Cyber Law (e.g., applicable statues of Title 10, 18, 32, 40, 44, 50)
2 Intermediate	• Follows established protocols and SOPs to monitor and support compliance with data security policies and relevant legal and regulatory requirements • Reviews organizational policy and procedural documents and articulates how current and future policies impact the organization when preparing legal documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery, etc.) • Reviews, interprets, and comments on current or proposed policies and regulations related to U.S. Cyber Law and National Cybersecurity Initiatives, including Presidential Directives and Executive Orders
3 Advanced	• Evaluates intelligence reporting principles, policies, procedures, and vehicles • Interprets legal terms by articulating advice and recommendations to executive decision makers to alleviate legal complications prior to implementing new changes in policies • Oversees the development of policy, programs and guidelines for implementation
4 Expert	• Advocates organization's official position in legal and legislative proceedings and coordinates with other legal agencies to ensure that the organization is making sound decisions that are based on both cybersecurity and legal policies

Strategic Planning and Policy Development	Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.
BEHAVIORAL INDICATORS	
1 Basic	• Collects information from stakeholders regarding system requirements and documents them for consideration by management into organizational planning reports • Consults organization-specific IA/IS policy criteria and assists in the identification of gaps and deficiencies; identifies any problems or issues encountered with the established policies or procedures by recording occurrences and reporting them to supervisors • Maintains existing SOPs, reference manuals, and information sources, and assists in the development of briefings that address policy affects and implications
2 Intermediate	• Prepares and delivers education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures • Defines, interprets, and implements policy related to customer and statutory requirements and translates/tailors these policies into a format that is clearly understood by a variety of audiences • Identifies compliance gaps and collaborates with colleagues and leadership to update organizational policies; researches new and emerging IA/IS technologies and applies it to policies • Researches congressional and executive mandates (e.g. guidelines, policies and US Codes) and statutes, technologies, trends, and current agency infrastructure and considers their applicability and implications for the agency when synthesizing findings and information into small intelligence briefings and reports
3 Advanced	• Formulates and provides recommendations to designated senior leadership regarding policy and regulatory status, the intersection of technology and policy, and impact of policy changes upon agencies • Reviews, analyzes, and provides recommendations on issuances by summarizing in a way that key stakeholders fully comprehend • Ensures compliance testing (e.g., policy, standards, guidelines) is included in the systems requirements planning and testing process; reports non-compliance in requirements and policy throughout all test phases • Establishes and maintains communications channels with stakeholders to coordinate and build consensus across an agency for proposed policy changes (including integration and implementation) • Advises on policy budget formulation and execution

Strategic Planning and Policy Development	Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.
BEHAVIORAL INDICATORS	
4 Expert	• Analyzes statutory requirements against existing directives to assess the degree of change necessary to comply with new requirements and acquisitions • Provides analysis on complex program related IT issues or problems to support the systems enterprise architecture lifecycle and oversees areas where new analytical techniques and policies must be developed, identified and evaluated to provide solutions • Oversees the development and implementation of policy and procedural controls covering security systems, contingency planning, compliance, and security education, training, and acquisitions • Serves as a cyber related policy expert on agency and interagency policy boards and provides input into the creation and enhancement of policies and procedures • Identifies and collaborates with key stakeholders to design and maintain cybersecurity strategies that outline the vision, mission, and goals that align with each organization's strategic plan

Education and Training	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.
BEHAVIORAL INDICATORS	
1 Basic	• Answers stakeholder and customer questions regarding simple concepts, material or tasks in an informal setting • Develops introductory cybersecurity training course content by writing procedures, creating course materials, and coordinating/training session(s) logistics • Assists in gathering course development material and content (e.g., research, resources) to prepare and support the delivery of security awareness training/briefings • Uses standard procedures to collect course evaluation data and reports findings to management • Collects training data for organization and FISMA requirements
2 Intermediate	• Develops and delivers cyber training, taking into account IT security policies and procedures to prepare and deliver/facilitate systems, network, and data security education and awareness briefings • Identifies public and private sector communication, training, and performance gaps by monitoring sector trends; identifies and recommends the development of training materials that address required, targeted training for gap closure • Designs, creates, delivers, maintains and facilitates training of various subject matters related to cybersecurity with minimal

Education and Training	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.
BEHAVIORAL INDICATORS	
	guidance
3 Advanced	• Gathers stakeholder interests and needs to determine content for training and uses Instructional Systems Design (ISD) methodologies to coach others in selecting the appropriate training modalities to address learning needs • Recommends additional and/or supplemental communication or training opportunities for existing and future trainings by evaluating previous, current, and proposed training efforts and comparing results with procedural, recommended, and organizational needs • Analyzes intended audience and lends ISD, forensic, IA/IS expertise to the development and delivery of training on complex topics • Communicates course requirements to vendors for course creation and reviews vendor generated course materials to ensure they coincide with training requirements and needs • Creates new training courses by developing outlines, story boards, content, material, and instruction method requirements, and coaches others in these activities; collaborates with subject matter experts to identify knowledge and training gaps
4 Expert	• Assesses technical and legal trends that will impact cybersecurity activities; designs and implements agency-wide security awareness training program • Coordinates with other agencies to develop integration plans for new training courses to be included into existing curricula • Analyzes annual reports and legal requirements of FISMA • Leads process improvement teams in training gaps analysis to determine training gaps within an organization; identifies additional training needs, synthesizes research and findings to present training needs to agency stakeholders, and develops strategic security awareness and training programs • Develops training performance metrics to determine effectiveness of training and training programs

Information Systems Security Operations (Information Systems Security Officer [ISSO])	Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.
BEHAVIORAL INDICATORS	
1 Basic	• Collects and maintains data needed to meet IA/IS reporting and/or Security Authorization • Keeps IA/IS documents and guidance compliant with new and/or revised policies by updating them as directed • Follows SOPs to conduct compliance monitoring and reports anomalies in enabled software, hardware, and/or firmware that may result in non-compliance with appropriate IT security guidelines or policies
2 Intermediate	• Prevents disclosure and protects the infrastructure by ensuring that inspections, tests, and reviews are coordinated for the network environment • Assesses operational impact of policy on the organization • Assists in the implementation of security policy by reviewing a new policy against all applicable agency and higher policies, directives, mandates, and laws to support compliance initiatives and recommending changes to senior leadership for minimizing risks • Performs risk mitigation actions • Uses IT security configuration guidelines, policies and procedures to assess compliance of IA/IS and IA/IS-enabled software, hardware, and firmware
3 Advanced	• Reviews a new policy against all applicable agency and higher policies, directives, mandates, and laws to recommend changes to senior leadership for minimizing risks • Supervises or manages protective or corrective measures when an incident or vulnerability is discovered by generating a solution, allocates the appropriate personnel to resolve the incident, and follows up to ensure the incident is resolved • Coordinates and builds consensus across an organization for security planning and IA/IS strategies, including the integration and implementation of these efforts and oversees compliance monitoring across the network environment • Verifies that IA requirements are integrated into the COOP for that system or agency and accurately identified in the computer environment operation procedures
4 Expert	• Establishes audit policy and reporting mechanisms for ensuring compliance with IA/IS standards by keeping current with IA/IS requirements • Analyzes identified security strategies by assessing them against the organization's needs and compliance guidelines and selects the best approach or practice for the enterprise • Leads the development of risk management by creating plans, procedures, protocols, and evaluation measures and ensuring

Information Systems Security Operations (Information Systems Security Officer [ISSO])	Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.
BEHAVIORAL INDICATORS	
	there are desired levels of enterprise-wide IA/IS • Oversees the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents • Strategically integrates operations, intelligence and security in support of mission requirements

Security Program Management (Chief Information Security Officer [CISO])	Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
BEHAVIORAL INDICATORS	
1 Basic	• Gathers information regarding data classification policies, laws, and guidance relevant to IA/IS and communicates it to others through basic written guidance • Cites and references policy regarding protection of Personally Identifiable Information (PII) and organizational sensitive data • Keeps data classification and management policies updated by staying current on any revisions and changing them as directed • Supports others in gathering information for technical documents (such as incident reports, findings from computer examinations, summaries and/or other situational awareness reports) • Participates in the implementation of security plans by disseminating plans and protocols to users, gaining feedback from users and stakeholders, and reporting findings through briefings
2 Intermediate	• Alerts management to issues with project implementation/execution and makes recommendations for improvements • Monitors information security programs, reviews reports, and reports critical issues to senior leadership • Assists in the implementation of privacy and security plans and objectives by identifying and mitigating problems and risks that may have adverse impact on the project or program • Uses best practice analysis principles and methods to interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's IA/IS program

Security Program Management (Chief Information Security Officer [CISO])	Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
BEHAVIORAL INDICATORS	
3 Advanced	• Implements security plans and objectives by monitoring progress, recommending solutions to barriers, and delegating tasks to personnel; coaches and/or advises others in these areas • Keeps abreast of new and emerging cybersecurity technologies, practices, and policies and synthesizes this information and collaborates with key stakeholders to construct alternative functional security strategies to address cyber related security concerns • Analyzes the effectiveness of the enterprises' security plans and safeguards (examining for full compliance against mandates) to ensure they provide the intended level of protection; advises CIOs or other leadership on risk levels of security posture • Evaluates the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisitions documents
4 Expert	• Conducts an effective enterprise continuity of operations program, and reduces overall organizational risk; identifies and prioritizes critical business functions and coordinates with stakeholders to establish programs and strategies that drive mission assurance • Ensures a coherent, coordinated, and holistic approach to security across the organization; evaluates the presence and adequacy of security measures proposed or provided by comparing them to requirements contained in acquisition documents • Interprets patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise IA/IS program • Oversees and coaches others in analysis of principles and methodologies for network systems management, systems performance monitoring, and network traffic analysis for de-conflicting cyber operations and activities • Analyzes cyber related security policies, legislation and regulatory requirements to develop detailed cyber operations plans which align to the mission of the organization and defines measurable criteria and metrics to monitor success

Appendix F: References

The table below displays the resources used in the creation of this report.

Table 41: References

Reference	Date	Location
Government Accountability Office - Cybersecurity Human Capital – Initiatives Need Better Planning and Coordination	November 2011	http://www.gao.gov/new.items/d128.pdf
Cyberspace Policy Review	2009	http://www.dhs.gov/publication/2009-cyberspace-policy-review
Comprehensive National Cybersecurity Initiative (CNCI)	January 2008	http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
2011 IT Workforce Capability Assessment Survey Results Report	May 2011	https://cio.gov/resources/document-library/

Homeland Security

National Cybersecurity Education Office (CEO)

Contact Information:

Robin "Montana" Williams, Director
Email: Robin.Williams@HQ.DHS.GOV
Phone: 703.235.5169

Edward W. Nyack
IT Workforce Assessment for Cybersecurity (ITWAC) Project Lead
Email: Edward.Nyack@hq.dhs.gov
Phone: 703.235.5294